



**G O B I E R N O
R E G I O N A L D E
L O S L A G O S**

Acción de Futuro

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

**PROCEDIMIENTO "CUMPLIMIENTO CON LAS POLÍTICAS -
NORMAS DE SEGURIDAD Y
VERIFICACIÓN DEL CUMPLIMIENTO TECNICO"**

CÓDIGO	SSI-A.18.02.02 SSI-A.18.02.03	CLASIFICACIÓN INFORMACIÓN		Reservada
			X	Uso Interno
				Pública
VERSIÓN	1.0	FECHA DE LA VERSIÓN	27-09-2019	
RESPONSABLE	Comité Seguridad de la Información.			

Código: SSI-A.18.02.02 SSI-A.18.02.03	CUMPLIMIENTO CON LAS POLÍTICAS - NORMAS DE SEGURIDAD Y VERIFICACIÓN DEL CUMPLIMIENTO TECNICO	
Versión: 1.0		
Fecha : 27-09-2019		
Página : 2 de 6		

Historial de modificaciones

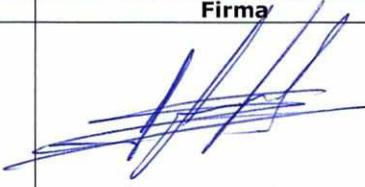
Creación/Modificaciones del Documento

Versión	Fecha de modificación	Autor	Motivo	Páginas modificadas	Firma
1.0	24-09-2019	Nicanor Bahamonde, Profesional Unidad Informática	Creación de la primera versión del procedimiento	Todas	

Revisiones

Versión	Fecha	Autor	Observación	Páginas	Firma
1.0	27-09-2019	Javier Soto Mancilla, Apoyo Profesional Depto. Finanzas	Sin observaciones	Todas	

Visto Bueno

Versión	Fecha	Encargado	Firma
1.0	17-10-2019	Oscar Alejandro Oyarzo Pérez, Encargado de Seguridad de la Información	
1.0	17-10-2019	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	Enviado por correo electrónico e instruida la publicación en intranet a la Unidad de Informática

Código: SSI-A.18.02.02 SSI-A.18.02.03	CUMPLIMIENTO CON LAS POLÍTICAS - NORMAS DE SEGURIDAD Y VERIFICACIÓN DEL CUMPLIMIENTO TECNICO	
Versión: 1.0		
Fecha : 27-09-2019		
Página : 3 de 6		

Contenido

1. Objetivo	4
2. Alcance o ámbito de aplicación interno	4
3. Roles y Responsabilidades.	4
4. Procedimiento	5
5. Documentos de referencia	5
6. Registros de control del procedimiento	5
7. Validez y gestión de documentos	6

Código: SSI-A.18.02.02 SSI-A.18.02.03	CUMPLIMIENTO CON LAS POLÍTICAS - NORMAS DE SEGURIDAD Y VERIFICACIÓN DEL CUMPLIMIENTO TECNICO	
Versión: 1.0		
Fecha : 27-09-2019		
Página : 4 de 6		

1. Objetivo

Permitir Verificar el cumplimiento con las políticas y normas de seguridad de la información del Gobierno Regional.

2. Alcance o ámbito de aplicación interno

El presente procedimiento, establecerá el procedimiento para verificar el cumplimiento con las políticas y normas de seguridad de la información del Gobierno Regional. Este procedimiento es aplicable a todos los sistemas de información del Gobierno Regional.

3. Roles y Responsabilidades.

ROLES	RESPONSABILIDADES
Jefe DAF	<ul style="list-style-type: none"> Asegurar que existan las condiciones, elementos, materiales y medidas de seguridad para que se pueda desarrollar correctamente la actividad.
Encargado de Seguridad de la Información	<ul style="list-style-type: none"> Responsable de velar por el cumplimiento de este procedimiento al interior del Servicio cuando corresponda. Responsable de la distribución de este documento y asegurar su incorporación a la base documentaria del servicio.
Comité Seguridad de la Información	<ul style="list-style-type: none"> Revisar controles y políticas del SSI vigentes, verificando su cumplimiento. Tomar medidas, si se encuentran deficiencias en la implementación de controles de Seguridad de la Información.
Encargado Unidad de Informática	<ul style="list-style-type: none"> Coordinar que se ejecute correctamente el procedimiento. Evaluar el conocimiento adquirido respecto al trabajo y designar al personal idóneo para la ejecución del mismo.

Código: SSI-A.18.02.02 SSI-A.18.02.03	CUMPLIMIENTO CON LAS POLÍTICAS - NORMAS DE SEGURIDAD Y VERIFICACIÓN DEL CUMPLIMIENTO TECNICO	
Versión: 1.0		
Fecha : 27-09-2019		
Página : 5 de 6		

4. Procedimiento

El comité de seguridad de la Información, debe revisar anualmente el cumplimiento de los procedimientos de Seguridad de la Información, así como velar por el cumplimiento por parte de los funcionarios y responsables involucrados en cada control o política respectiva.

El comité de Seguridad de la información al detectar faltas en el cumplimiento de normas, procedimientos y políticas de seguridad de la información, deberá identificar las causas del incumplimiento, posteriormente el comité tendrá que evaluar las acciones y medidas para lograr el cumplimiento de las normas que tienen dificultad en su cumplimiento. Para mitigar los riesgos asociados a la seguridad de la información el comité de seguridad de la información debe implementar acciones correctivas adecuadas y revisar la acción correctiva tomada para verificar su efectividad e identificar cualquier tipo de deficiencias y falencias.

Además, una vez al año se deberán revisar los controles existentes en este Gobierno Regional, verificando que todos cumplan con las normas ISO en materias de seguridad de la información.

Respecto a la revisión de cumplimiento técnico se debe realizar revisiones mediante pruebas para verificar penetraciones o evaluaciones de vulnerabilidad en los sistemas de información que se ajusten a las normas y política de Seguridad de la Información previamente validadas por el Comité de Seguridad de este Gobierno Regional, las que deberán ser documentadas. Estas deberán realizarse a lo menos una vez al año.

5. 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.13.01.02	Seguridad de los Servicios de 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.

6. Registros de control del procedimiento.

- a) Informe Reporte de "Revisión en busca de penetraciones o vulnerabilidades de sistemas de información"
- b) Acta de reunión Comité de Seguridad de la Información.

Código: SSI-A.18.02.02 SSI-A.18.02.03	CUMPLIMIENTO CON LAS POLÍTICAS - NORMAS DE SEGURIDAD Y VERIFICACIÓN DEL CUMPLIMIENTO TECNICO	
Versión: 1.0		
Fecha : 27-09-2019		
Página : 6 de 6		

7. Validez y gestión de documentos

Este documento es válido desde la fecha de su aprobación.

El responsable de este documento es el Comité de Seguridad de la Información, que debe verificar, y si es necesario actualizar el documento, por lo menos una vez cada tres años.

	Aprobado Por	
		
Oscar Alejandro Oyarzo Pérez Encargado de Seguridad de la Información		
17 de octubre de 2019		