GOBIERNO REGIONAL DE LOS LAGOS

Acción de Futuro

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

PROCEDIMIENTO "CONTROLES CONTRA CÓDIGO MALICIOSO"

CÓDIGO	**SSI-A.12.02.01**	**CLASIFICACIÓN INFORMACIÓN**		**Reservada**
			X	**Uso Interno**
				Pública
VERSIÓN	1.0	**FECHA DE LA VERSIÓN**	24-09-2019	
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	24-09-2019	Eduardo Madrid Osorio, Encargado Unidad de Informática	Creación de la primera versión del procedimiento	Todas	

Revisiones

Versión	Fecha	Autor	Observación	Páginas	Firma
1.0	26-09-2019	Javier Soto Mancilla, Profesional Depto. Finanzas	Sin observaciones	Todas	

Visto Bueno

Versión	Fecha	Encargado	Firma
1.0	05-11-2019	Oscar Alejandro Oyarzo Pérez, Encargado de Seguridad de la Información	
1.0	05-11-2019	Alejandro Montaña Ampuero, Administrador Regional Gobierno Regional de Los Lagos	GOBIERNO REGIONAL ADMINISTRADOR 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

Contenido

1. Objetivo.

Definir las medidas de prevención, detección, corrección y concientización frente a las amenazas causadas por códigos maliciosos.

2. Alcance o ámbito de aplicación interno.

Este procedimiento es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros, es decir, proveedores, que presten servicios al Gobierno Regional de Los Lagos.

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos y se requiere tomar precauciones para evitar y detectar la introducción de códigos de programación maliciosos y códigos con capacidad de reproducción y distribución automática no autorizados para la protección de la integridad del software y de la información que sustentan.

El código malicioso es código informático que provoca infracciones de seguridad para dañar un sistema informático. El malware se refiere específicamente a software malicioso, pero el código malicioso incluye además scripts de sitios web (applets de Java, controles de ActiveX, contenido insertado, plug-ins, lenguajes de scripts u otros lenguajes de programación en páginas web y correo electrónico) que pueden aprovechar vulnerabilidades con el fin de descargar un malware.

El software y los recursos de tratamiento de información son vulnerables a la introducción de software malicioso como virus informáticos, gusanos de la red, caballos de troya y bombas lógicas.

Los funcionarios deben estar al tanto de los peligros de los códigos maliciosos como el robo y destrucción de la información o daños e inutilización de los sistemas de la organización.

Para evitar la inyección de código malicioso a la red del servicio se combinarán controles tecnológicos (antivirus), lista blanca (softwares permitidos) y con medidas no técnicas (educación, concienciación y formación).

3. Roles y Responsabilidades.

ROLES	RESPONSABILIDADES
Encargado de Seguridad de la Información	• Velar por el cumplimiento del Procedimiento de Control contra código malicioso.
Encargado de la Unidad de Informática	• Realizar la Actualización del Procedimiento de Control contra código malicioso cuando se requiera. • Entregar al usuario un equipo debidamente protegido con antivirus y con los programas establecidos en lista blanca para el uso de la institución.
Usuarios Finales	• Conocer el Procedimiento de Control contra código malicioso.

4. Procedimiento.

a) Encargado de la Unidad Informática prepara el equipo computacional que usará el funcionario / honorario con sus debidos programas (en lista blanca) para el desempeño laboral y protección contra virus con su base de datos antivirus actualizada.
b) Como medida extra se instala un cliente de respaldo (veeam agent) cuya función dependiendo del grado es respaldar carpetas o el equipo completo.
c) Validación de los softwares para control contra código malicioso y protección, respaldo y restauración de la información.
d) Si la validación y puesta en marcha están OK, se cierra el proceso y se entrega el equipo al funcionario / honorario.
e) Si la validación no es satisfactoria se repite el procedimiento hasta que su puesta en marcha y validación estén OK.

4.1. Documentos de referencia.

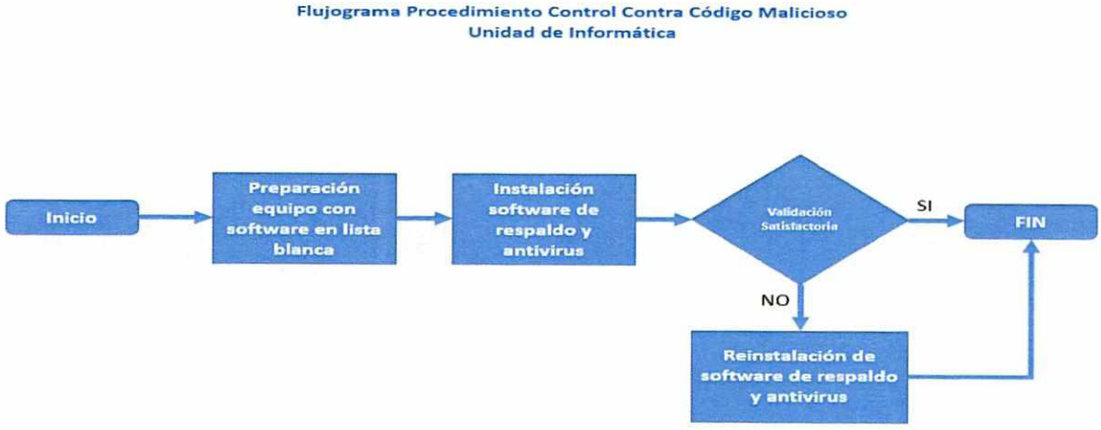
En la siguiente tabla, se presentan los documentos que se han utilizado como referencia, para la formulación del presente manual de procedimientos.

Código	Descripción
SSI-A.05.01.01	Política de Seguridad de la Información
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. Registros de control del procedimiento.

a) Pantallazo escritorio para verificar el correcto funcionamiento del software de respaldo y protección contra virus.
b) Pantallazo panel de control => características y programas para verificar la instalación del software de respaldo y protección contra virus.

4.3. Diagrama de Proceso.



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**
05 de Noviembre de 2019