PROCEDIMIENTO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN ACUERDOS CON EL PROVEEDOR

Nch 27001/2013 Control

A.15.01.02
A.15.01.03
A.15.02.01
A.15.02.02

CONTROL DE CAMBIOS:

Versión	Fecha	Responsable	Acción
1.0	Noviembre - 2019	SANDRA PÉREZ GUZMÁN	Elaborado

Validado:

Comité Seguridad de La Información

Funcionario	Integrante Comité	Firma
Luis Patricio Acum Salinas	Encargado de Unidad de Informática	
Paola Hermosilla Bucarey	Encargado de Departamento Jurídico	
Cesar Pérez Sepúlveda	Encargado de Dep. de Finanzas	
Wilson Monzón Riquelme	Jefe Div. de Presupuesto e Inversión Regional	
Heidi Machmar Hernández	Jefe Div. Planificación y Desarrollo Regional	
Carlos Ovando Hernández	Jefe Div. de Administración y Finanzas	
Eduardo Fagalde Ampuero	Jefe Div. de Desarrollo Social y Humano	
Ernesto Espinoza Navarrete	Jefe Div. de Fomento Productivo e Industria	
Alejandro Paredes Zieballe	Administrador Regional	
Rodrigo Aravena Bustamante	Coordinador de PMG de la Institución.	

GOBIERNO REGIONAL INTENDENTE REGION DE LOS RIOS

CESAR ASENJO JERÉZ
INTENDENTE
GOBIERNO REGIONAL DE LOS RÍOS

Contenido

1. OBJETIVO 4
2. ALCANCE O AMBITO DE APLICACIÓN DEL PROCEDIMIENTO 4
3. MARCO REFERENCIAL 4
4. ROLES Y RESPONSABILIDADES 5
5. DEFINICIÓN DEL PROCEDIMIENTO 5
   - 5.1 ABORDAR LA SEGURIDAD DENTRO DE LOS ACUERDOS CON EL PROVEEDOR 5
   - 5.2 CADENA DE SUMINISTROS DE LA TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN 6
   - 5.3 MONITOREO Y REVISIÓN DE LOS SERVICIOS DEL PROVEEDOR. 6
   - 5.4 GESTIÓN DE CAMBIOS A LOS SERVICIOS DEL PROVEEDOR. 6
6. REVISIONES 7
7. REGISTROS DE OPERACIÓN 7

1. OBJETIVO

El objetivo del presente procedimiento es establecer los lineamientos bajo los cuales se debe proceder en los acuerdos a contratos con el proveedor o terceros, mediante los cuales dichos externos tengan acceso a activos de información del Gobierno Regional de Los Ríos.

Con ello, asegurar que la información a la que se tenga acceso será tratada de forma reservada y cumpliendo con los estándares de seguridad establecidos por la institución, así como las posibles sanciones que pudieran dar lugar frente al incumplimiento de las mismas.

2. ALCANCE O AMBITO DE APLICACIÓN DEL PROCEDIMIENTO

El presente procedimiento es aplicable a todos aquellos funcionarios del Gobierno Regional que debido a la naturaleza de sus funciones suscriban acuerdos o contratos de prestación de servicios con terceros o con proveedores, así como para aquellos externos que tengan acceso a activos de información de la institución en cualquier etapa de la prestación.

3. MARCO REFERENCIAL

Decreto Supremo N°83 del Ministerio Secretaría General de la Presidencia, el cual "Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos"; Sistema de Gestión de Seguridad de la Información (NCh 27001, NCh 27002), perteneciente al Programa de Mejoramiento de la Gestión del Ministerio de Hacienda a través de la Dirección de Presupuestos (DIPRES) y que se rige por la Ley N° 19.553 y sus modificaciones, la cual "Concede Asignación de Modernización y otros Beneficios que se indica".

Política de Seguridad de la Información aprobada por el Jefe de Servicio mediante Resolución Exenta N° 1676 con fecha 26 de octubre de 2018.

Política de Seguridad de la Información para Relaciones con Proveedores, aprobada por el jefe de servicio mediante Resolución Exenta N° 2141 de fecha 19 de noviembre de 2019.

4. ROLES Y RESPONSABILIDADES

Responsable	Rol	Funciones
Jefe de Servicio	Liderar la implementación del presente Procedimiento de.	✓ Aprobar el documento. ✓ Autorizar los recursos necesarios para su implementación.
Comité de Seguridad de la Información	Aprobar y coordinar la implementación del procedimiento.	✓ Aprobar el procedimiento. ✓ Coordinar su correcta implementación y seguimiento.
Encargado de Seguridad de la Información	Gestionar e informar al comité acerca de la implementación del procedimiento.	✓ Informar de manera periódica al comité de seguridad de la información del grado de avance en la implementación del procedimiento.
Encargado Unidad de Informática	Liderar la implementación del procedimiento desde el área técnica.	✓ Liderar la implementación del procedimiento desde el área técnica.
Jefes de división	Difundir el procedimiento	✓ Difundir entre los funcionarios el presente procedimiento.
Funcionarios	Conocer e implementar el procedimiento	✓ Conocer e implementar el procedimiento en los acuerdos o contratos con el proveedor.

El conocimiento, aceptación y uso del presente documento por parte de todos los involucrados es de responsabilidad del Encargado de Seguridad de la Información del Gobierno Regional de Los Ríos.

5. DEFINICIÓN DEL PROCEDIMIENTO

5.1 ABORDAR LA SEGURIDAD DENTRO DE LOS ACUERDOS CON EL PROVEEDOR

Como forma de minimizar los riesgos de seguridad de la información en los accesos de terceros y en los acuerdos con el proveedor, se debe identificar y establecer las reglas de seguridad en los contratos considerando los siguientes aspectos:

- ✓ Definir el tipo de proveedor y de accesos que tendrá a la información institucional, de acuerdo a ello, se deben establecer y acordar previamente las condiciones para el resguardo de los activos de información.
- ✓ Identificar claramente al proveedor y el tipo de prestación o servicio que está otorgando, especialmente aquellos que tengan relación directa con servicios de TI.
- ✓ Definir el tipo de acceso y los permisos y/o privilegios que les serán otorgados y los tiempos de conexión o acceso.
- ✓ Monitorear el cumplimiento de los acuerdos en seguridad de la información durante todo el proceso.
- ✓ Establecer obligaciones aplicables al proveedor.
- ✓ Manejo de incidentes por parte del funcionario contraparte o perteneciente al área de informática de la institución.

5.2 CADENA DE SUMINISTROS DE LA TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN.

En la cadena de suministros de tecnologías de información, se deben tener presente los siguientes aspectos de seguridad:

- ✓ Definir y exigir que se cumpla con los requisitos de seguridad aplicables a la adquisición de tecnologías de información, es decir, sistemas, software, aplicaciones, infraestructura, etc.
- ✓ En caso de subcontrataciones, se debe asegurar que los requisitos de seguridad de la información se apliquen a toda la cadena de suministro.
- ✓ En el caso de partes, piezas y componentes comprados a otros proveedores, se debe asegurar que los requisitos de seguridad sean aplicados de igual forma a toda la cadena de suministros.

5.3 MONITOREO Y REVISIÓN DE LOS SERVICIOS DEL PROVEEDOR.

- ✓ Se debe monitorear de forma periódica y mientras los servicios contratados se ejecuten, el cumplimiento de los acuerdos de seguridad de la información con el proveedor.
- ✓ Revisar los aspectos de seguridad de la información de las relaciones que tiene el proveedor con sus propios proveedores.
- ✓ Identificar y resolver cualquier problema de seguridad de la información que se presente durante o después de la prestación de servicios.

5.4 GESTIÓN DE CAMBIOS A LOS SERVICIOS DEL PROVEEDOR.

En el caso de los servicios provistos por terceros tanto en desarrollo como mantención, actualización y cambios de software, sistemas o infraestructura de redes, se deberá, en lo general aplicar las restricciones anunciadas en el Procedimiento de Control de Cambios Internos y Externos aprobado por el Comité de Seguridad de la Información con fecha septiembre de 2019 y aplicables a esa situación, además de ello se deberá tener especial cuidado en los siguientes aspectos:

- ✓ Registrar y aprobar todo cambio realizado en las instalaciones relacionadas con infraestructura tecnológica y de redes, llámese cambio de equipos, cambios y mejoras en las redes, uso de nuevas tecnologías, adopción de nuevos productos, cambio de proveedores, etc.
- ✓ Mantener comunicación fluida con el proveedor para evitar cambios no autorizados, manifestando en los documentos contractuales las condiciones y restricciones frente a los cambios o actualizaciones disponibles.
- ✓ Proponer cambios a los acuerdos con el proveedor que impliquen mejoras al acuerdo inicial en el sentido de operatividad y satisfacción del funcionamiento del sistema.

6. REVISIONES

El presente documento ha sido revisado y aprobado por el comité de seguridad de la información del Gobierno Regional de Los Ríos, en concordancia con lo dispuesto en el Sistema de Gestión de Seguridad de la Información, por lo cual deberá ser revisado, al menos, una vez cada un año de acuerdo al grado de cumplimiento.

7. REGISTROS DE OPERACIÓN

Los pasos para dar cumplimiento a los dispuesto en el presente procedimiento serán de responsabilidad del Encargado de Seguridad de la Información de la Institución, quién, en conjunto con el encargado del área informática y el proveedor, definirán de acuerdo al tipo de servicio y el grado de acceso a la información o la criticidad de los sistemas involucrados, la forma más conveniente de incorporar, monitorear y supervisar que se dé cumplimiento a los requisitos de seguridad en los acuerdos o contratos de prestación de servicios externos.

El proveedor o tercero prestador de servicios debe tener acceso y conocer la Política de Seguridad de la Información para las Relaciones con los Proveedores aprobada por el jefe de servicio mediante Resolución Exenta N° 2141 de fecha 19 de noviembre de 2019, así como los procedimientos que de ella emanen. Dicha obligatoriedad se hará efectiva mediante memorándum del Encargado de Seguridad de la Información Institucional hacia los funcionarios que son parte de los contratos o acuerdos con terceros y a la unidad de adquisiciones para asegurar que se incorpore dentro de los contratos o bases de licitación un enunciado que contenga lo descrito en el presente párrafo.