Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.15.01.01	Política de seguridad de la información para las relaciones con el proveedor.

2019

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR

Control de versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
15-06-2016	1.0	Marcelo Aliaga Q. Liliana Reyes G.	Elaboración de Política.
05-10-2016	1.1	Marcelo Aliaga Q. Liliana Reyes G.	Modificación de texto y configuración de documentos.
17-10-2016	1.2	Marcelo Aliaga Q. Liliana Reyes G.	Modificación formato de portada, tabla control de versiones, marcos de imágenes, objetivo de control.
13-10-2017	2.0	Marcelo Aliaga Q. Liliana Reyes G.	Modificación de contenidos en base a documento "Estrategia de Trabajo SSI 2017". Se incorporan títulos: Alcance, Objetivo, Roles y responsabilidades, Mecanismo de difusión, Evaluación y revisión. Se incorpora en pág. 4 punto 6 Evaluación y revisión (...) *"No obstante, podrá revisarse cuando la situación amerite o la autoridad lo disponga".*
11-10-2018	3.0	Jorge Romero V. Solange Godoy C.	Actualización de política incorporando título Definiciones. Sección 2 se incorporó punto acerca de la protección de los activos Se complementó sección 3

			Sección 4 se desagregan roles y responsabilidades.
14-10-2019	4.0	Jorge Romero Vargas Solange Godoy Carrera	Se cambia estructura a documento, de acuerdo a guía metodológica. Se modifica en Roles y responsabilidades, agrupando División/Comisión/Unidad En Definiciones/Prestación de servicios al Ministerio, se incorpora "Las comunicaciones con el proveedor...". En Control se modifica nombre Jefatura DAG y pie de firma de Jefe de Tecnologías de la Información.

1. Introducción

El Ministerio Secretaría General de la Presidencia dispone del presente documento, "Política de Seguridad de la Información para las relaciones con el Proveedor", como parte integrante del sistema de seguridad de la información. En específico, se enmarca en el cumplimiento de la NCH ISO 27001, que propone como requisito de control:

Control A.15.01.01 Política de seguridad de la información para las relaciones con el proveedor
"Se deben acordar y documentar, junto con el Proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del Proveedor a los activos de la organización".
Requisito control A.15.01.01 NCH ISO 27001-2013

2. Alcance

Este documento se aplicará a las acciones que desarrollan externos que prestan servicios en el Ministerio y que pertenezcan a empresas proveedoras de servicios. Esta política garantizará la seguridad de los accesos a los sistemas de información de los proveedores y mitigar alguna contingencia de pérdida tanto de información como de equipos, dispositivos, entre otros. Así también, a todos los usuarios de este Ministerio, ya sean funcionarios de planta, contrata, honorarios, asesores, alumnos en práctica y terceros que puedan estar prestando servicios en el Ministerio y que requieran el uso de sistemas y servicios de información.

3. Objetivo

El presente documento denominado "Política de Seguridad de la Información para las Relaciones con el Proveedor", tiene como objetivo:

- Definir las reglas básicas para la relación con los Proveedores del Ministerio
- Mejorar las relaciones interacciones con los Proveedores del Ministerio
- Facilitar la comunicación entre los Proveedores y el Ministerio
- Mantener la Seguridad de Información con proveedores
- Garantizar la protección de los activos del Ministerio que son accesibles a los proveedores

4. Roles y responsabilidades

Independiente del cargo/rol que se desempeñe, del nivel jerárquico del que se goce y de la modalidad bajo la cual se esté contratado, es responsabilidad de todo el personal de este Ministerio conocer y dar debido cumplimiento a este documento, asimismo, es responsabilidad de:

- **Jefes/as de División/Comisión/Unidad:** La aplicación de la política, en los funcionarios y trabajadores, así también del cumplimiento, promover y supervisar el estricto apego a esta norma.
- **Encargado de Seguridad de la Información:** La definición de normas y procedimientos para la identificación de los riesgos asociados con el acceso a los activos del Ministerio, esto por parte de los proveedores.
- **Comité de Seguridad de la Información:** La revisión, además velar por el cumplimiento, actualización y difusión de esta Política.

- **Proveedores:** los proveedores deben dar estricto cumplimiento a esta política y procedimientos que deriven de ésta.
- **Personal externo:** deben dar estricto cumplimiento a esta política y procedimientos que deriven de ésta

5. Mecanismo de difusión

Es responsabilidad del Comité de Seguridad de la Información difundir este documento el que deberá permanecer en la Intranet institucional a disposición de todo el personal del Ministerio.

6. Evaluación y revisión

El tiempo de evaluación y revisión estándar para este documento, será cada dos años. No obstante, podrá revisarse cuando la situación lo amerite o la autoridad así lo disponga. El Encargado de Seguridad de la Información, enviará documentación con los cambios y/o actualizaciones de la Política. El Comité de Seguridad de la Información revisará, observará y aprobará.

7. Definiciones

Toda la información que sea valiosa para el Ministerio incluye diversos tipos de activos relacionados con la organización (edificios, instalaciones, equipamiento) y personal, activos que se relacionan con los sistemas de información (equipos, software, comunicaciones), activos que se relacionan con la información (datos, soporte).

Es responsabilidad de todos los funcionarios que poseen y/o tengan bajo responsabilidad información de la que no es propietario, aplicar las medidas de seguridad correspondiente para el resguardo de esta información.

- **Prestación de servicios al Ministerio**
    - Los proveedores sólo podrán desarrollar para el Ministerio, aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios. De este modo, se entenderá que todas las actividades desarrolladas para el Ministerio por personal perteneciente a empresas proveedoras se encuadran en los contratos de provisión de servicios que vinculan al Ministerio con estos proveedores.
    - Las actividades desarrolladas por el personal perteneciente a empresas proveedoras se realizarán de acuerdo a lo establecido en el correspondiente contrato de provisión de servicios, así como a las normas y procedimientos establecidos a tal efecto entre el Ministerio y el proveedor correspondiente.
    - La empresa proveedora deberá asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio como de manera transversal en materia de seguridad de la información, para lo cual deberá asegurar, al menos, de que todo el personal asociado al servicio conoce y se compromete a cumplir las presentes Políticas de Seguridad.
    - Cualquier tipo de intercambio de información que se produzca entre el Ministerio y las empresas proveedoras se entenderá que ha sido realizado dentro del marco establecido por el contrato de provisión de servicios correspondiente, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho contrato.

- Las comunicaciones con el proveedor se deberían realizar mediante correo electrónico institucional y en caso de sostener reuniones se debería generar un acta formal. No se debería utilizar mensajería móvil o acuerdos mediante comunicación telefónica.
- El área se seguridad informática centraliza los esfuerzos globales de protección de los activos del Ministerio, a fin de asegurar el correcto funcionamiento de las tecnologías de la información que soportan los procesos de la organización.

- **Confidencialidad en la Información**
  - El personal externo que tenga acceso a información del Ministerio deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información del Ministerio a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos para tal efecto por el Ministerio.
  - Se evitará la revelación, modificación, destrucción o mal uso de la información cualquiera sea el soporte en que se encuentre contenida.
  - Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior, información confidencial, salvo que esté debidamente autorizado.
  - Se minimizará el número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.
  - En relación a la utilización de agendas de contactos, de las herramientas ofimáticas dispuestas por el Ministerio, el personal únicamente introducirá datos personales como nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. Ningún colaborador de proyectos, trabajos puntuales, etc., deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada al Ministerio.
  - El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en el artículo 197 del Código Penal, que puede dar derecho a exigir compensaciones. Para garantizar la seguridad de los Datos de Carácter Personal albergados en ficheros automatizados, el personal que pertenece a empresas proveedoras deberá observar las siguientes normas de actuación, además de las consideraciones ya mencionadas:
    - El personal sólo podrá crear archivos temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo.
    - No se albergarán datos de carácter personal en las unidades locales de disco.
    - La salida de soportes informáticos que con tengan datos de carácter personal, fuera de las dependencias en las que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable del fichero y se realizará según el procedimiento definido.
    - Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido al personal autorizado.

8. Control

Elaborado por: Jorge Romero Vargas Solange Godoy Carrera
Jorge N. Romero V.
Fecha: 14-10-2019

Comité de Seguridad de la Información del Ministerio Secretaría General de la Presidencia

Texia Gutiérrez Inostroza Jefa División Administración General	Pamela Ávila Rubio Jefa Unidad de Control de Gestión
	Pamela Ávila R.
Fecha: 14-10-2019	Fecha: 14-10-2019

Anamaría Verdugo Marchese Abogada Asesora CSI	Jorge Romero Vargas Jefe Unidad de Tecnologías de la Información Oficial de Seguridad de la Información
A. Verdugo M.	Jorge N. Romero V.
Fecha: 14-10-2019	Fecha: 14-10-2019