Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.12.01.04	Separación de los ambientes de desarrollo, prueba y operacionales
A.12.02.01	Controles contra códigos maliciosos
A.12.06.02	Restricciones sobre la instalación de software

Control de versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
30-05-2019	1.0	Jorge Romero Vargas Solange Godoy Carrera	Elaboración de Documento

1. Introducción

El Ministerio Secretaría General de la Presidencia dispone del presente documento, "Política de Seguridad de las Operaciones", 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.12.01.04 Separación de los ambientes de desarrollo, prueba y operacionales

"Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación".

- Requisito de control A.12.01.04 NCH ISO 27001-2013

Control A.12.02.01 Controles contra códigos maliciosos

"Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios".

- Requisito de control A.12.02.01 NCH ISO 27001-2013

Control A.12.06.02 Restricciones sobre la instalación de software

"Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios".

- Requisito de control A.12.06.02 NCH ISO 27001-2013

2. Alcance

Esta política se aplicará a todos los usuarios de este Ministerio, también a alumnos en práctica y terceros que puedan prestar servicios, para lo cual requieran utilizar sistemas y medios tecnológicos de información.

3. Objetivo

El objetivo de esta política es normar funciones que corresponden directamente al resguardo de la información contenida en los equipos asignados a cada trabajador del Ministerio, por lo que mantener una separación de ambientes de funciones y ambientes lógicos, así como monitorear y controlar los sistemas contra códigos maliciosos, mediante un antivirus y el estricto control de instalación de software, mitigan riesgos de contaminación con aplicativos poco confiables.

4. Roles y responsabilidades

Independientemente 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 esta Política

- **Jefe Unidad de Tecnologías de la Información**

  Su responsabilidad será velar por las acciones que deban realizar para la mitigación de riesgos de la información, separando los ambientes de desarrollo, controlar, prevención contra códigos maliciosos y restringir los accesos para la instalación de software no autorizados.

- **Encargado de Seguridad de la Información**
  Monitorear el debido cumplimiento de esta norma en la Unidad de Tecnología de la Información, así como realizar revisiones periódicas del cumplimiento de esta norma.
- **Jefes/as División, Comisión, Unidad**
  Su responsabilidad es conocer y concientizar entre los trabajadores a su cargo el cumplimiento de las reglas que rigen para la instalación de software de personas que no cuentan con autorización.
- **Funcionarios/Trabajadores**
  Su responsabilidad es estar informado de lo contenido en esta norma y dar estricto cumplimiento a control sobre la instalación de software.

5. Mecanismo de difusión

Es responsabilidad del Comité de Seguridad de la Información, la difusión de este Política, la que deberá ser enviada por correo electrónico a cada trabajador y permanecer a disposición de todos los usuarios de este Ministerio en la Intranet institucional.

6. Evaluación y revisión

El tiempo de evaluación y revisión estándar de esta Política, será cada dos años o las veces que la autoridad lo determine. El Encargado de Seguridad de la Información informará en sesión del Comité de Seguridad de la Información los cambios y/o actualizaciones, por lo que el Comité de Seguridad de la Información revisará, observará y aprobará.

7. Definiciones

- **Control A.12.01.04 Separación de los ambientes de desarrollo, prueba y operacionales**
  La separación de funciones y ambientes lógicos es una forma de mitigar riesgos que se puedan ocasionar de manera accidental o por mal uso de sistema, debido a la existencia de entornos más críticos, por cuanto se deberá separar los ambientes de producción, desarrollo y mantenimiento de los sistemas de información.
  La separación de los equipos y los sistemas operativos se deberán diferenciar.
  El ambiente de producción no deberá estar incorporado al ambiente de desarrollo, en el que existe la instalación de los sistemas informáticos para el desarrollo de aplicaciones, así como tampoco el ambiente de pruebas (Testing/QA).
  Estos entornos, desarrollo, pruebas y producción deberán contener: separación de red, separación de las bases de datos y separación de los roles de seguridad.

- **Control A.12.02.01 Controles contra códigos maliciosos**
  La Unidad de Tecnología de la Información deberá monitorear que todos los sistemas del servicio sean analizados por un antivirus, el que se deberá ejecutar antes y después de abrir un archivo. Este proceso deberá ser automático.
  Los trabajadores del Ministerio no deberán hacer uso de un software que no haya sido proporcionado o autorizado por la Unidad de Tecnología de la Información.

Los usuarios deberán verificar que, tanto la información como el medio de almacenamiento no estén infectados de algún software malicioso, para lo anterior deberán ejecutar el software antivirus que esté autorizado por la Unidad especializada en la materia.
Los archivos que se reciban por personas externas y también por personal institucional, que se relacionen con software, bases de datos, documentos, etc., y que deban ser descomprimidos, se deberá verificar que estén libres de virus.
Ningún usuario del Ministerio deberá descargar software de sistemas, sistemas de correo electrónico o redes de comunicación externa sin la autorización de la jefatura directa y de la Unidad de Tecnología de la Información.
Si los usuarios detectan que el equipo computacional se encuentra infectado deberá tomar contacto inmediato con la Unidad de Tecnología de la Información.
Los trabajadores del Ministerio no deberán cambiar ni eliminar las configuraciones de seguridad para la detección o prevención de la propagación de un virus.
Cualquier medio removible y otro medio de almacenamiento que se encuentre infectado no deberán ser utilizados hasta que el virus haya sido erradicado
Ningún trabajador del Ministerio deberá intentar eliminar un virus por sí sólo, debe contactarse con la Unidad de tecnología de la Información para el retiro inmediato del equipo.

- **Control A.12.06.02 Restricciones sobre la instalación de software**

  El control en la instalación de software busca mitigar riesgos de aplicativos desconocidos y poco confiable, debido al acceso a las redes del Ministerio, a las que se puede acceder a través de internet, correo electrónico entre otros, por lo que la Unidad de Tecnología de la Información deberá restringir los permisos o acceso, sólo los usuarios autorizados y capacitados podrán instalar software en los equipos tecnológicos proporcionado por el Ministerio.

9. Control

Elaborado por: Jorge Romero Vargas Solange Godoy Carrera
Jorge N. Romero V.
Fecha: 28-06-2019

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: 28-06-2019	Fecha: 28-06-2019

Anamaría Verdugo Marchese Abogada Asesora CSI	Jorge Romero Vargas Jefe Unidad de Tecnología de la Información Oficial de Seguridad de la Información
A. Verdugo M	Jorge N. Romero V.
Fecha: 28-06-2019	Fecha: 28-06-2019