Controles NCH ISO 27001:2013 Relacionados
Deriva de Política de Seguridad de las Operaciones

CONTROL	NOMBRE
A.12.02.01	Controles contra código malicioso

PROCEDIMIENTO DE CONTROLES CONTRA CÓDIGOS MALICIOSOS

Control de versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
30-09-2019	1.0	Jorge Romero Vargas Solange Godoy Carrera	Elaboración de procedimiento
24-09-2021	1.1	Jorge Romero	Mejoras en formulario CCM-03. Actualización de sección firmantes. Mejoras en la redacción.

1. Introducción

El Ministerio Secretaría General de la Presidencia, dispone del presente documento denominado "Procedimiento de Controles contra Códigos Maliciosos", como parte integrante del Sistema de Seguridad de la Información. En específico, se enmarca en el cumplimiento de la Norma Chilena ISO 27001, que propone como requisito de control:

Control A.12.02.01 Controles contra códigos malicioso

"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

2. Objetivo

El objetivo de este procedimiento es entregar los lineamientos adoptados para controlar, y a la vez mitigar cualquier riesgo asociado a códigos maliciosos que puedan poner en riesgo la seguridad de la información en el Ministerio Secretaría General de la Presidencia.

3. Alcance

Este procedimiento se aplicará a los sistemas operativos, además de todos los trabajadores, alumnos en práctica y terceros que puedan estar prestando servicios en el Ministerio y que requieran autorización para el uso de equipamiento tecnológico.

4. Roles y Responsabilidades

Independiente del cargo/rol que se desempeñe, el 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 el debido cumplimiento a este procedimiento, asimismo, es responsabilidad de:

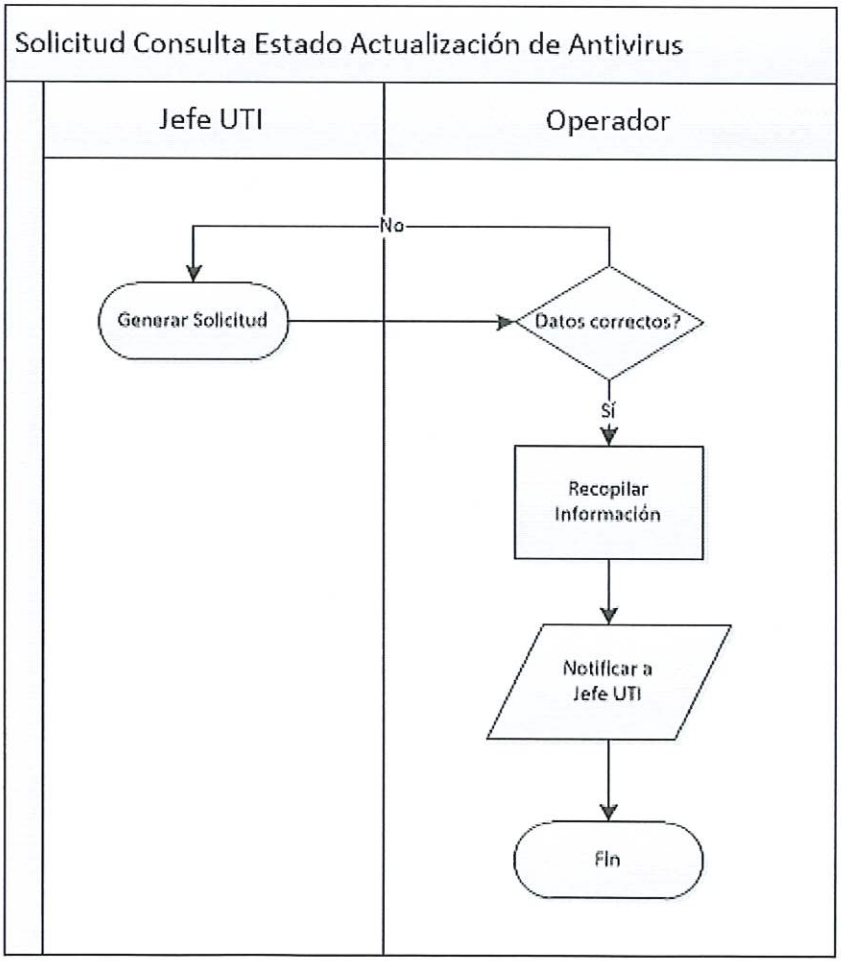
- **Jefe Unidad de Tecnologías de la Información (Jefe UTI)**
  Velar por las acciones que se deban realizar para la mitigación de riesgos de la información, separando los ambientes de desarrollo, controlando y aplicando medidas de prevención contra la ejecución de códigos malicioso, como también restringir los accesos para la instalación de software no autorizados.
- **Encargado de Seguridad de la Información**
  Monitoreo permanente del cumplimiento de este procedimiento en la Unidad de Tecnologías de la Información, así como realizar revisiones periódicas de su cumplimiento.
- **Jefes/as División, Comisión, Unidad**
  Conocer y concientizar entre los trabajadores a su cargo el cumplimiento de este procedimiento.
- **Funcionarios/Trabajadores**
  Estar informado del contenido de este procedimiento y dar estricto cumplimiento al mismo.
- **Operador**
  Funcionario / Trabajador de la Unidad de Tecnologías de la Información que participa en el proceso para ejecutar una operación específica.

5. Definiciones y modo de operación

El Procedimiento de controles contra códigos maliciosos contempla los siguientes subprocesos:

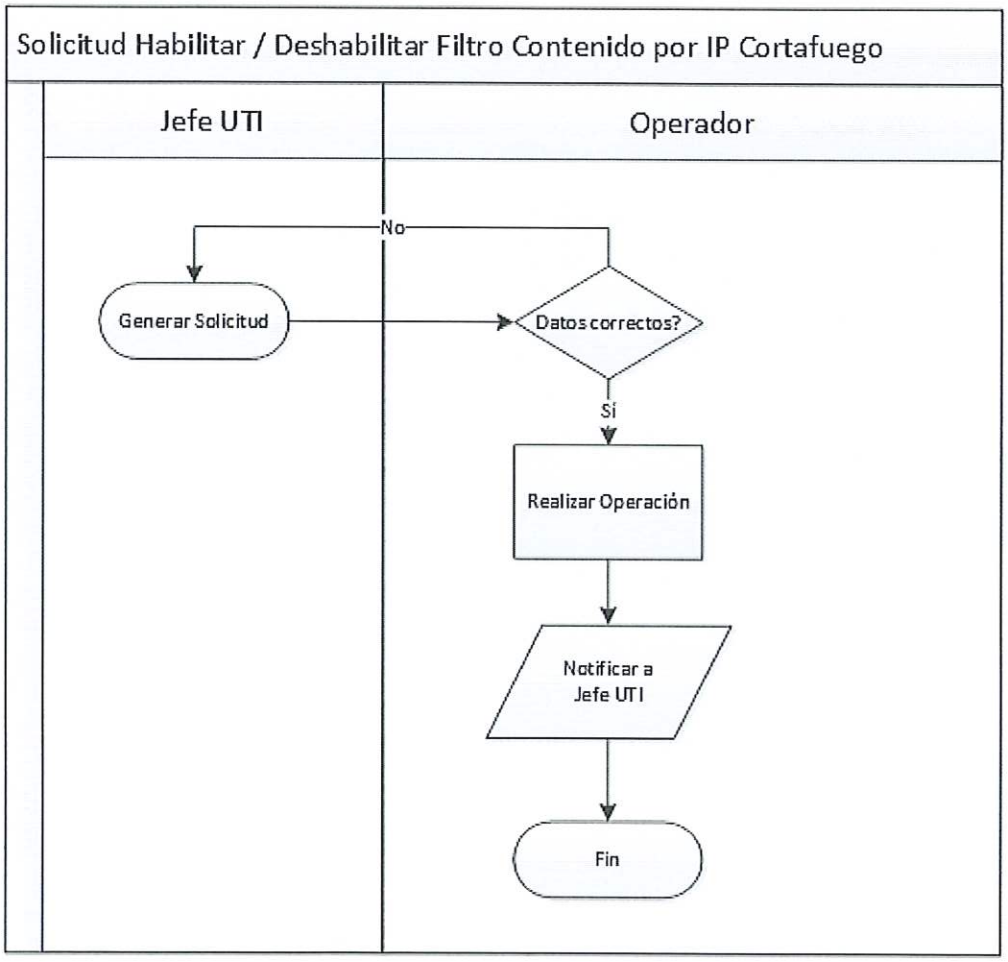
- Solicitud Consulta Estado Actualización de Antivirus
- Solicitud Habilitar / Deshabilitar Filtro Contenido por IP Cortafuego
- Solicitud Habilitar / Deshabilitar Filtro Contenido por Patrón Antispam
- Solicitud Habilitar / Deshabilitar Filtro Contenido por IP Antispam

Subproceso: Solicitud Consulta Estado Actualización de Antivirus.
Control: A.12.02.01 Controles contra códigos malicioso.
El Jefe de la Unidad de Tecnologías de la Información deberá realizar un control de actualización del antivirus de la Institución. Para ello, deberá completar una solicitud la cual será enviada al operador quien proporcionará la fecha de última actualización de este y alguna observación de ser necesaria.



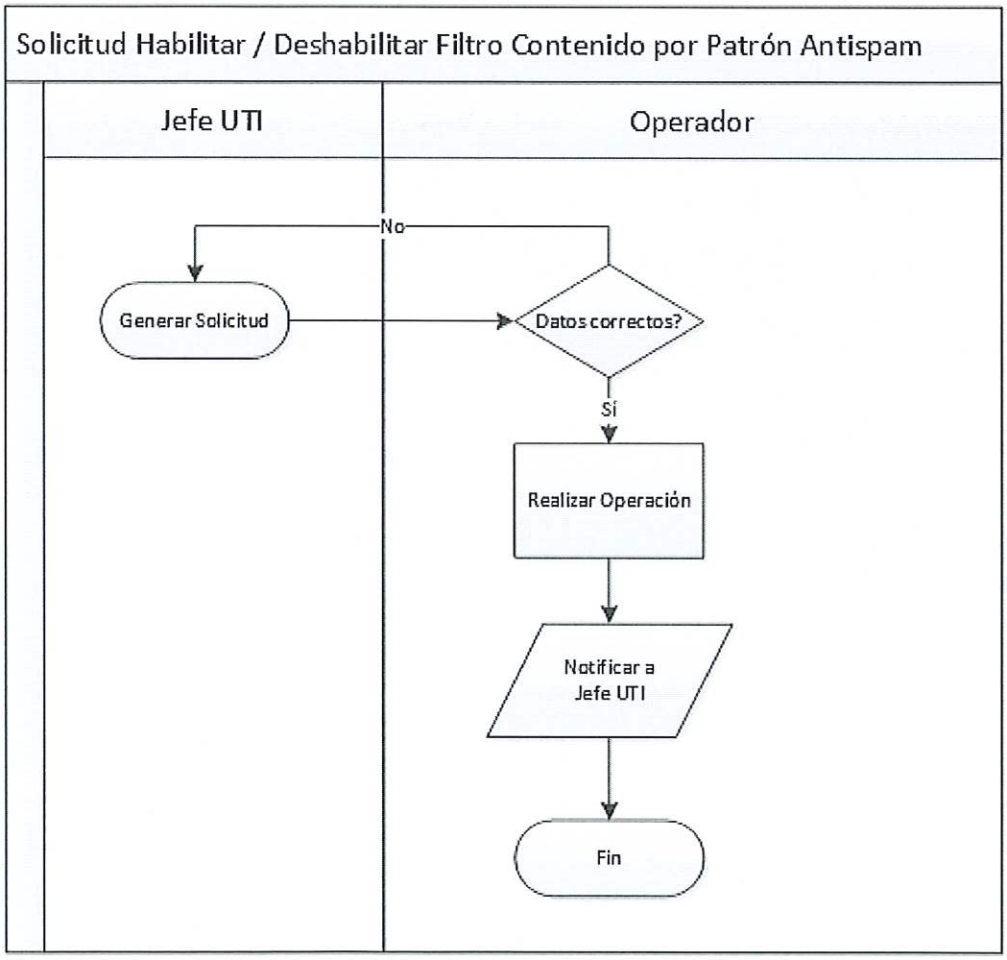
Descripción de actividades: El Jefe UTI debe generar una Solicitud Consulta Estado Actualización de Antivirus, la cual será enviada al Operador quien deberá validar los datos y realizará la recopilación de información notificando posteriormente al Jefe UTI.

Subproceso: Solicitud Habilitar / Deshabilitar Filtro Contenido por IP Cortafuego.
Control: A.12.02.01 Controles contra códigos malicioso.
El Jefe de la Unidad de Tecnologías de la Información podrá solicitar habilitar / deshabilitar filtro de contenido por IP en el cortafuego de la institución. Para ello deberá completar una solicitud indicando la dirección IP y un comentario que justifique dicha operación a realizar por el operador.



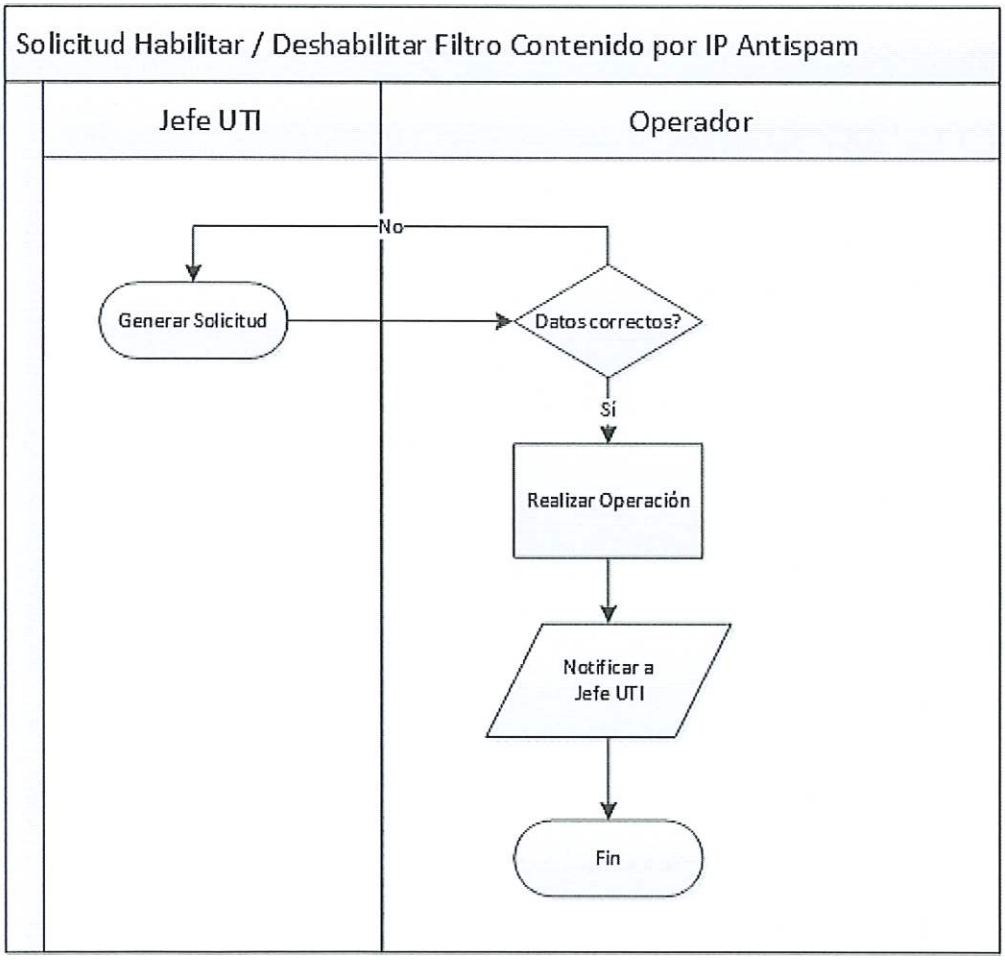
Descripción de Actividades: El Jefe UTI genera una Solicitud Habilitar / Deshabilitar Filtro Contenido por IP Cortafuego, la cual será enviada al Operador quien deberá validar los datos y realizará la operación notificando posteriormente al Jefe UTI.

Subproceso: Solicitud Habilitar / Deshabilitar Filtro Contenido por Patrón Antispam.
Control: A.12.02.01 Controles contra códigos malicioso.
El Jefe de la Unidad de Tecnologías de la Información podrá solicitar habilitar / deshabilitar filtro de contenido por patrón en el dispositivo antispam de la institución. Para ello deberá completar una solicitud indicando el patrón y un comentario que justifique dicha operación a realizar por el operador. Deberá indicar si el patrón es aplicable al asunto, encabezado o cuerpo del correo electrónico. Esta solicitud podrá permitir realizar operaciones de habilitación o deshabilitación. Podrá determinar, además, si es un correo de entrada o salida, como también si se deberá bloquear o enviar a cuarentena.



Descripción de Actividades: El Jefe UTI genera una Solicitud Habilitar / Deshabilitar Filtro Contenido por Patrón Antispam, la cual será enviada al Operador quien validará los datos y realizará la operación notificando posteriormente al Jefe UTI.

Subproceso: Solicitud Habilitar / Deshabilitar Filtro Contenido por IP Antispam.
Control: A.12.02.01 Controles contra códigos malicioso.
El Jefe de la Unidad de Tecnologías de la Información podrá solicitar habilitar / deshabilitar filtro de contenido por IP en el dispositivo Antispam de la institución. Para ello deberá completar una solicitud indicando la dirección IP y un comentario que justifique dicha operación a realizar por el operador.



Descripción de Actividades: El Jefe UTI podrá generar una Solicitud Habilitar / Deshabilitar Filtro Contenido por IP Antispam, la cual será enviada al Operador quien deberá validar los datos y realizará la operación, notificando posteriormente al Jefe UTI.

6. Registro de Operación

Subproceso: Solicitud Habilitar / Deshabilitar Filtro Contenido por Patrón Antispam.
Control: A.12.02.01 Controles contra códigos malicioso.
Formulario: CCM-01.

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

CCM-01
Unidad de Tecnologías de la Información
Solicitud habilitar/deshabilitar filtro contenido por patrón antispam
A.12.02.01

Fecha: ☐

Patrón: ☐ Habilitar: ☐ Deshabilitar: ☐

Comentario:

☐

	Bloquear	**Cuarentena**
Entrada		
Salida		

Asunto ☐
Encabezado ☐
Cuerpo ☐

Operado por

Nombre: ☐
RUT: ☐

_____
Firma

Autorizado por Jefe Unidad de Tecnologías de la Información (UTI):

Nombre: ☐
RUT: ☐

_____
Firma

Subproceso: Solicitud Habilitar / Deshabilitar Filtro Contenido por IP Antispam.
Control: A.12.02.01 Controles contra códigos malicioso.
Formulario: CCM-02

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

CCM-02
Unidad de Tecnologías de la Información
Solicitud habilitar/deshabilitar filtro contenido por IP antispam
A.12.02.01

Fecha: _____

IP: _____

Comentario:

_____

Operado por

Nombre: _____

RUT: _____

_____
Firma

Autorizado por Jefe Unidad de Tecnologías de la Información (UTI)

Nombre: _____

RUT: _____

_____
Firma

Subproceso: Solicitud Habilitar / Deshabilitar Filtro Contenido por IP Cortafuego.
Control: A.12.02.01 Controles contra códigos malicioso.
Formulario: CCM-03.

CCM-03
Unidad de Tecnologías de la Información
Solicitud habilitación/deshabilitación filtro contenido por IP en corta fuego
A.12.02.01

☐ Habilitar ☐ Deshabilitar **Fecha:**

IP	Comentario o Justificación

Operado por

Nombre:

RUT:

Firma

Autorizado por Jefe Unidad de Tecnologías de la Información (UTI):

Nombre:

RUT:

Observaciones:

Firma

Subproceso: Solicitud Consulta Estado Actualización de Antivirus.
Control: A.12.02.01 Controles contra códigos malicioso.
Formulario: CCM-04.

Ministerio Secretaría General de la Presidencia
Gobierno de Chile

CCM-04
Unidad de Tecnologías de la Información
Consulta estado de actualización de antivirus

A.12.02.01

Fecha:

Solicitante Jefe Unidad de Tecnologías de la Información (UTI)

Nombre:

RUT:

Firma

Antivirus

Fecha última actualización

Observaciones:

Operado por

Nombre:

RUT:

Firma

7. Documentos relacionados

Este procedimiento está relacionado directamente con controles contenidos en la Política de Seguridad de las Operaciones vigentes, del Ministerio Secretaría General de la Presidencia.

8. Indicador

El indicador mide la ejecución del procedimiento y subprocesos en base a las solicitudes que se ingresan y son atendidas en general.

Meta anual: 80%
Fórmula de cálculo:

(N° de solicitudes realizadas / N° de solicitud recibidas) *100

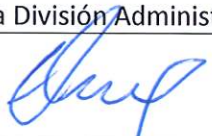
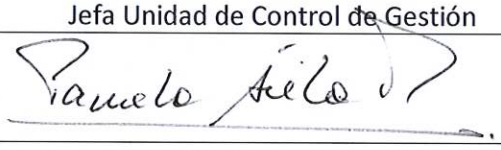
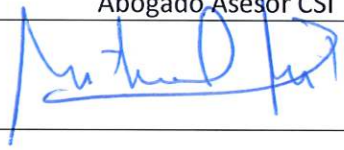
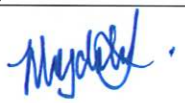
Plazo de ejecución: < 24 horas de recibida la solicitud

9. Control

Elaborado por: Jorge Romero Vargas

Fecha: 24-09-2021

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

Texia Gutiérrez Inostroza Jefa División Administración General	Pamela Ávila Rubio Jefa Unidad de Control de Gestión
	
Michael Mc Donnell Bernabé Abogado Asesor CSI	Magdalena Ortega Puebla Abogado Asesor Gabinete del Subsecretario
	
Loreto Alarcón Godoy Abogado Asesor Comisión de Integridad y Transparencia	Carlos Gómez Cruz Jefe División de Gobierno Digital
	

Jorge Romero Vargas Oficial de Seguridad de la Información Jefe Unidad de Tecnologías de la Información

Fecha: 24-09-2021