Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.13.01.01	Controles de red
A.13.01.02	Seguridad de los servicios de red
A.13.01.03	Separación de las redes
A.13.02.02	Acuerdos sobre transferencia de información
A.13.02.03	Mensajería electrónica

Control de versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
30-05-2019	1.0	Jorge Romero Vargas Solange Godoy Carrera	Elaboración de Documento
30-10-2020	1.1	Jorge Romero Vargas	Incorpora restricciones en el uso de dispositivos de comunicaciones de propiedad personal dentro de la institución, bloqueo por zona geográfica, uso de aplicaciones especiales en la red interna de tipo bridge, proxys o vpn personales. Incluye autenticación de dos factores para administración.
24-09-2021	1.2	Jorge Romero	Actualización en sección firmantes. Mejora en la redacción del documento en lo correspondiente a grupos de distribución institucionales.
10-11-2023	1.3	Jorge Romero	Actualización en sección firmantes. Modifica Jefe Unidad de Tecnologías de la Información por Encargado Área de Tecnologías de la Información. Modifica Unidad de Tecnologías de la Información por Área de Tecnologías de la Información. Incorpora lenguaje inclusivo en el documento. Aumenta tamaño de envío de correos a 15 Megabytes.

1. Introducción

El Ministerio Secretaría General de la Presidencia dispone del presente documento, "Política de Seguridad en las Redes y Comunicaciones", como parte integrante del sistema de seguridad de la información. En específico, se enmarca en el cumplimiento del NCH ISO 27001, que propone como requisitos de control:

Control A.13.01.01 Controles de red

"Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones".

- Requisito de control A.13.01.01, NCH ISO 27001-2013.

Control A.13.01.02 Seguridad de los servicios de red

"Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros".

- Requisito de control A.13.01.02, NCH ISO 27001-2013

Control A.13.01.03 Separación de las redes

"Los grupos de servicios de la información, usuarios/as y sistemas de información se deben separar en redes".

- Requisito de control A.13.01.03, NCH ISO 27001-2013

Control A.13.02.02 Acuerdos sobre transferencia de información

"Los acuerdos deben abarcar la transferencia segura de la información del negocio entre las organizaciones y terceros".

- Requisito de control A.13.02.02, NCH ISO 27001-2013

Control A.13.02.03 Mensajería electrónica

"La información involucrada en la mensajería electrónica debe ser debidamente protegida".

- Requisito de control A.13.02.03, NCH ISO 27001-2013

2. Alcance

Esta política se aplicará a todas las instalaciones y equipamientos que sean utilizados para el funcionamiento de la seguridad perimetral de este Ministerio, además de todos los/las funcionarios/as o trabajadores, alumnos en práctica y terceros que puedan estar prestando servicios en el Ministerio.

3. Objetivo

El objetivo de esta norma es aplicar al Ministerio controles o herramientas que permitan la seguridad de la información, para lo cual se controlará el acceso a los sistemas y aplicativos, reforzando la seguridad de los servicios de red con que cuente el servicio, separando dichas redes para minimizar riesgos en los dominios de red, así como la formalización de acuerdos que tengan relación con la entrega de información crítica o sensible, y que esta no sea mal utilizada por terceros. Asimismo, mantener un nivel alto de protección y monitoreo en todo lo concerniente a mensajería electrónica.

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 el debido cumplimiento a este procedimiento, asimismo, es responsabilidad de:

- **Encargado/a de redes y seguridad**
  Mantener un constante monitoreo a las redes de comunicación del Ministerio, implementando controles que permitan mitigar cualquier alteración en las redes de los sistemas de operación.
- **Encargado/a Área de Tecnologías de la Información**
  Verificar los recursos informáticos, tecnológicos y redes para el resguardo de la información ministerial.
- **Encargado/a de Seguridad de la Información**
  Velar por el apego de la institución a esta política y realizar revisiones periódicas al sistema de red.
- **Comité de Seguridad de la Información**
  Difundir y mantener actualizada esta norma.
- **Jefes/as de División, Comisión, Unidad**
  Difundir entre sus trabajadores las instrucciones de esta norma, resguardando con ello, los servicios de red, gestionando los acuerdos, si lo requiere, de la transferencia de información y velar por el buen uso de la mensajería electrónica.
- **Funcionarios/as y Trabajadores**
  Cumplir con las instrucciones impartidas por esta política en cuanto a la transferencia segura de información y el uso adecuado de la mensajería electrónica.

5. Mecanismos de difusión

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

6. Evaluación y revisión

El tiempo de evaluación y revisión estándar para esta política, será en un plazo máximo de dos años. No obstante, podrá revisarse cuando la situación lo amerite o la autoridad así lo disponga. El/la encargado/a de seguridad de la información informará en sesión del Comité de seguridad de la información los cambios y/o actualizaciones de esta norma. El Comité de seguridad de la información la revisará, observará y aprobará esta política según la normativa vigente y lineamientos establecidos por la institución.

7. Definiciones

Control A.13.01.01 Controles de red

El encargado de redes y seguridad deberá manejar y controlar adecuadamente las redes ministeriales para la debida protección de la información. Se deberán implementar controles para garantizar la seguridad de la información en las redes. Además, la protección de los servicios conectados de acceso no autorizados, para lo que se deberá considerar:

- La separación de la responsabilidad operacional de las redes de las operaciones informática.
- Se deberá establecer responsabilidades y procedimientos para la gestión del equipo remoto.
- Se deberán implementar controles para resguardar la confidencialidad e integridad de la data que se encuentra en las redes del Ministerio o inalámbricas, y proyectar los sistemas y aplicaciones conectados.
- Se deberán aplicar registros de ingreso y monitoreo, para permitir el registro de las acciones de seguridad.
- Las actividades deberán estar coordinadas para la optimización del servicio al Ministerio y asegurar que los controles se apliquen por medio de la infraestructura de procesamiento de la información.

Está estrictamente prohibido la Incorporación de otros dispositivos de comunicaciones de propiedad personal dentro de la red tales como BAM (Banda Ancha Móvil), AP (Access Point), Router, Switch, Mini Switch, Repetidores de señal y otros que no estén autorizados por el Área de Tecnologías de la Información.

El/la funcionario/a no deberá realizar ningún tipo de cambio en la estructura de conexión de red aplicada en su computador institucional. Tampoco podrá realizar escaneos de la red, ni ejecución de aplicativos que puedan afectar el rendimiento y disponibilidad de esta.

Está estrictamente prohibido el uso de aplicativos de tipo Bridge, Proxy o VPN personales.

El Área de Tecnologías de la Información aplicará como medida mitigadora, ante ataques informáticos, la realización de bloqueos por zona geográfica en cada uno de los portales o aplicaciones que administra.

Cada funcionario/a parte de la administración de servicios en la nube, deberá contar con una autenticación de dos factores.

La implementación de servicios en la nube deberá contar con una separación de ambientes ya sea a través de cuentas y otro mecanismo que permita mitigar riesgos de seguridad.

Control A.13.01.02 Seguridad de los servicios de red

Los/las usuarios/as del Ministerio Secretaría General de la Presidencia deberán tener acceso a la red, a través de una identificación de usuario/a y una contraseña única y personal, que deberá tener un mínimo de 8 caracteres, y que se deberá cambiar cada 90 días.

Se recomienda no copiar información sensible o crítica en dispositivos móviles. Los/las usuarios/as que cuenten con dispositivos móviles, deberán mantenerlos con clave inicial de bloqueo. Es responsabilidad de cada trabajador que la información no quede expuesta ante un mal uso o pérdida del dispositivo.

El uso del correo electrónico institucional deberá ser solo para el cumplimiento de las tareas propias del servicio. No se recomienda la utilización o el ingreso a correos personales a través de la red de internet ministerial. La conectividad fuera del Ministerio, por razones del servicio, recomienda privilegiar accesos seguros o bien, reducirlos al mínimo posible, entendiendo que servicios gratuitos de conectividad inalámbrica podrían ser intervenidos.

Los dispositivos como routers, firewall, switch, deberán tener contraseñas y sólo los/las funcionarios/as especializados del ministerio tendrán acceso remoto a estos equipos.

Esta estrictamente prohibida la impresión, publicación o divulgación de claves de acceso wifi a personas que no correspondan a la institución. No obstante, existirá una red de visitas, la cual podrá dar apoyo en conectividad de internet a participantes de reuniones que requieran hacer uso de este recurso para actividades relacionadas a la institución.

Control A.13.01.03 Separación de las redes

La separación de las redes se deberá hacer en los equipos de ruta a través de la configuración de la nómina de control de acceso, y las configuraciones que sean necesarias en los equipos de comunicaciones.

La conexión a redes inalámbricas, por restricciones de los equipos comunicacionales no se deberán conectar a red fija.

Los/las usuarios/as y servicios deberán estar separados lógicamente en unidades organizacionales o dominios a través de VLANS.

Control A.13.02.02 Acuerdos sobre transferencia de información

Se deberán implementar planes o guías que se relacionen con la transferencia de información, lo que permitirá mitigar riesgos en la seguridad. Se deberá aplicar el cifrado en las comunicaciones, así como la validación de identidad. Si existieran proveedores que prestan servicio al Ministerio y que deban acceder a información crítica o sensible, se deberá dar acceso

con herramientas que consideren criptografía de cifrado robusto y que evite cualquier tipo de amenaza a la seguridad de la información. Será necesario contar con un acuerdo formal entre el proveedor y la institución el cual proteja la divulgación de datos, mala utilización de esta o que se pueda revelar mediante un proceso de transferencia de información.

Control A.13.02.03 Mensajería electrónica y otros recursos de internet

No está permitido el uso del servicio Internet para escuchar radio o sintonizar canales de televisión, redes sociales, salvo autorización expresa de la jefatura directa y que por la naturaleza de sus funciones dentro de la institución lo amerite. No se permitirá el envío de correos electrónicos de un tamaño que exceda los 15 Megabytes. No está permitido el uso de software de tipo "p2p" o cualquier otro medio para compartir archivos por medio de Internet que no sea el proporcionado por la institución.

El/la funcionario/a deberá almacenar información de carácter institucional exclusivamente en su computador, carpetas compartidas y/o almacenamiento en la nube, recursos que la institución proporciona a cada funcionario/a para facilitar la accesibilidad, resguardo y trabajo colaborativo. Esto será administrado por el Área de Tecnologías de la Información.

El acceso a material pornográfico se encuentra inhabilitado para toda la institución y en cualquiera de sus medios. Los recursos correspondientes a música, video juegos y todo lo que no se relacione directamente con las tareas habituales de el/la funcionario/a se encuentra restringido.

El sistema de correo electrónico es una herramienta de trabajo que el Ministerio pone a disposición de los usuarios/as. Por esta razón, la información que se intercambie por este medio deberá restringirse a propósitos institucionales.

El Área de Tecnologías de la Información no realizará respaldos de los correos en las carpetas locales de los usuarios/as, siendo responsabilidad de éstos hacerlo.

Cada usuario/a deberá mantener bajo reserva su clave de acceso a la red institucional, la que permitirá el ingreso al correo electrónico, entre otros recursos.

El/la usuario/a deberá abstenerse de transmitir información confidencial o reservada por este medio, dado que no está garantizada la confidencialidad de los textos enviados a Internet, a menos que estos sean encriptados.

El correo electrónico institucional será administrado por el Área de Tecnologías de la Información siguiendo el patrón de creación [InicialPrimerNombre][PrimerApellido]@[dominio institucional].gob.cl y en casos de duplicidad de cuentas [InicialPrimerNombre][PrimerApellido][InicialSegundoApellido]@[dominio institucional].gob.cl. Este patrón de correo será considerado como el oficial de la Institución, manteniendo su debida disponibilidad, resguardo y respaldo de la información.

Las personas que ingresan a realizar su práctica profesional al Ministerio se les creará un correo electrónico de practica [NúmeroCorrelativoDeCreación]@[dominio institucional].gob.cl, el cuál será para ser utilizado en la institución. El Área de Tecnología de la Información deberá restringir el envío de información fuera de la institución.

El uso del listado de direcciones de correos electrónicos es para consulta y uso exclusivo dentro del Ministerio, y está prohibido difundir este listado por cualquier medio electrónico o impreso para propósitos que no sean de uso institucional.

El área de soporte gestionará y creará correos genéricos a petición expresa de la jefatura correspondiente.

Cada trabajador del servicio deberá tener acceso a su correo electrónico de forma remota. Asimismo, el Área de Tecnologías de la Información no otorgará soporte de los servicios de correo que no sea proporcionado por la institución para el desarrollo de sus tareas.

El correo electrónico es proporcionado por la Institución como herramienta de trabajo propia de las funciones de cada funcionario/a, el cual no debe ser utilizado para autenticación en redes sociales u otras plataformas digitales, realizar o recibir notificaciones de transferencias electrónicas de bancos, comercio o cualquier otra operación en línea a través de internet. Por otra parte, con el fin de mitigar riesgos de contaminación por este tipo de canal de comunicación desde el exterior, quedará inhabilitada la recepción de todo tipo de correos electrónicos que no correspondan al ejercicio del funcionario/a. Existirán excepciones que por la naturaleza del cargo serán habilitadas para cumplir su ejercicio o función pública dentro de la institución.

Existirá un encargado responsable de grupo de distribución de correos electrónicos, quien podrá autorizar la incorporación o remoción de correos electrónicos institucional en estos para la función que se requiera. Los grupos de distribución podrán recibir información desde correos electrónicos internos y excepcionalmente se podrá habilitar el acceso para recibir información desde correos electrónicos no institucionales, lo cual deberá estar debidamente justificado.

La creación de cuentas genéricas deberá estar debidamente justificada, y existirá un responsable propietario de administración. La cuenta podrá ser delegada en uno o más funcionarios/as, no obstante, siempre deberá mantenerse un responsable de su contenido y administración.

El pie de firma del correo electrónico del funcionario/a será autorizado y descrito por la Unidad de Gestión y Desarrollo de las Personas, perteneciente a la División de Administración General. El Área de Tecnologías de las Información estará facultada para realizar la configuración en el cliente de correo del computador asignado al funcionario o colaborador.

No deberá ser enviada información de autenticación de aplicaciones de la institución a grupos de distribución o cuentas de correo electrónicos de esta.

En caso de requerir un almacenamiento histórico de notificaciones de aplicaciones en ambientes de producción, estas deben ser direccionadas únicamente a una cuenta genérica destinada a este fin. Las notificaciones deben ser dirigidas a quienes corresponda dentro de los destinatarios. No obstante, en ambientes de desarrollo o pruebas podrán ser dirigidas al encargado del desarrollo de la aplicación para corroborar su correcta realización.

8. Control

Elaborado por: Jorge Romero Vargas
Jorge V. Romero V.
Fecha: 10-11-2023

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

Samir Toro Garrido Jefe División Administración General	Pamela Ávila Rubio Jefa Unidad de Control de Gestión
	Pamela Ávila R.
Sebastián Aguirre Ulloa Asesor División Jurídico-Legislativa	Christian Valenzuela Lorca Jefe Gabinete de la Subsecretaria
S. Aguirre	
Fabiola Vidal Oyarzún Asesor Comisión de Integridad y Transparencia	José Inostroza Lara Jefe División de Gobierno Digital

Jorge Romero Vargas Oficial de Seguridad de la Información Encargado Área de Tecnologías de la Información
Jorge V. Romero V.
Fecha: 10-11-2023