Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.18.01.01	Identificación de la legislación vigente y los requisitos contractuales
A.18.01.03	Protección de los registros
A.18.02.01	Revisión independiente de la seguridad de la información
A.18.02.02	Cumplimiento con las políticas y normas de seguridad
A.18.02.03	Verificación del cumplimiento técnico

Control de Versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
01-07-2019	1.0	Jorge Romero V. Solange Godoy C.	Elaboración de documentación
03-10-2023	1.1	Jorge Romero V.	Actualización sección firmantes. Actualiza Unidad de Tecnologías de la Información por Área de Tecnologías de la Información. Actualiza Jefe/a Unidad de Tecnologías de la Información por Encargado/a Área de Tecnologías de la Información. Mejoras en la redacción del documento. Incorpora lenguaje inclusivo en el documento.

1. Introducción

El Ministerio Secretaría General de la Presidencia dispone del presente documento, "Política de Lineamientos Normativos", 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.18.01.01 Identificación de la legislación vigente y los requisitos contractuales

"Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización".

- Requisito control A.18.01.01 NCH ISO 27001-2013

Control A.18.01.03 Protección de los registros

"Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio".

- Requisito control A.18.01.03 NCH ISO 27001-2013

Control A.18.02.01 Revisión independiente de la seguridad de la información

"El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos".

- Requisitos control A.18.02.01 NCH ISO 27001-2013

Control A.18.02.02 Cumplimiento con las políticas y normas de seguridad

"Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes".

- Requisito control A.18.02.02 NCH ISO 27001-2013

Control A.18.02.03 Verificación del cumplimiento técnico

"Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización".

- Requisito control A.18.02.03 NCH ISO 27001-2013

2. Alcance

La política de lineamientos normativos deberá abarcar la identificación y el cumplimiento de todas las obligaciones legales, regulatorias y contractuales relacionadas con la seguridad de la

información; la implementación de medidas de protección para los registros organizacionales contra la pérdida, destrucción y acceso no autorizado, acorde con los requisitos aplicables; la realización de revisiones independientes para asegurar la efectividad de la gestión de la seguridad de la información; la supervisión por parte de las jefaturas de centros de responsabilidad para dar cumplimiento a políticas y procedimientos de seguridad en sus respectivas áreas; y la verificación técnica regular de los sistemas de información para garantizar su alineación con las políticas y normas de seguridad vigentes. Esta política deberá ser integral, contemplando todas las facetas del manejo de información y aplicarse consistentemente a través de toda la institución para mantener la confiabilidad, integridad y disponibilidad de los datos.

3. Objetivo

La política de lineamientos normativos tiene como objetivo principal establecer un marco coherente y eficiente para la creación y gestión de normas dentro de la institución. Buscando asegurar la consistencia, claridad y cumplimiento legal de las regulaciones, facilitando su comprensión y aplicación. Además, promover la eficiencia operativa, la adaptabilidad a cambios, y la mejora continua, manteniendo un control riguroso y entrega de resultado. Este enfoque ayuda a alinear las normativas con los objetivos y valores de la entidad, garantizando su efectividad y relevancia.

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 la Política de Lineamientos Normativos, asimismo, es responsabilidad de:

- **Encargado/a área de Tecnologías de la Información**
  Asegurar que todos los sistemas de TI estén en conformidad con los requisitos legales, regulatorios y contractuales. Mantener un registro actualizado de dichos requisitos y garantizar que las configuraciones y operaciones de los sistemas de TI cumplan con ellos. Además, es su deber proteger los registros electrónicos, facilitar las auditorías y revisiones independientes de seguridad de la información, asegurar que las operaciones de TI cumplan regularmente con las políticas y normas de seguridad y conducir auditorías internas para verificar el cumplimiento técnico de los sistemas de TI. Este rol colabora estrechamente con el Encargado/a de Seguridad de la Información y reporta al Comité de Seguridad de la Información para fortalecer la postura de seguridad organizacional.
- **Encargado/a de Seguridad de la Información**
  Implementar y mantener controles para proteger los registros de información según lo exige la legislación y los requerimientos contractuales. Coordinar la revisión independiente de la seguridad de la información y asegurar que se actúe sobre las recomendaciones resultantes. Verificar y asegurar el cumplimiento de las políticas y normas de seguridad en la organización.

- **Comité de Seguridad de la Información**
  Supervisar el programa de cumplimiento normativo y protección de registros. Asegurar que las revisiones independientes se realicen adecuadamente. Revisar y aprobar los cambios en las políticas y procedimientos de seguridad derivados de las revisiones de cumplimiento.
- **Jefes/as de División, Comisión, Unidad**
  Garantizar que las políticas y procedimientos de seguridad de la información se apliquen y se respeten dentro de sus respectivas áreas. Colaborar con las revisiones periódicas y revisiones independientes, proporcionando el acceso necesario a la información y a los recursos. Monitorear y reportar el cumplimiento de los controles de seguridad en su ámbito, y gestionar las acciones correctivas necesarias.
- **Funcionarios/as o Trabajadores**
  Conocer y comprender los requisitos de cumplimiento relevantes para sus roles y las consecuencias de la no conformidad. Mantener la seguridad y la integridad de los registros de información con los que trabajan diariamente. Participar y cooperar en las revisiones y auditorías de seguridad, así como en los programas de formación y concienciación.

5. Mecanismo de difusión

Es responsabilidad del Comité de Seguridad de la Información difundir esta política, publicándose en la intranet institucional a disposición de todo el personal del Ministerio.

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.18.01.01 Identificación de la legislación vigente y los requisitos contractuales

El Ministerio deberá establecer un método sistemático para la identificación y comprensión cabal del marco jurídico pertinente, abarcando leyes, normativas y requisitos contractuales específicos a la seguridad de la información. Este proceso sistemático incluirá el acceso a bases de datos jurídicas actualizadas, la interacción regular con abogados y expertos en cumplimiento, así como la utilización de listas de verificación exhaustivas que garanticen la cobertura integral de todas las áreas de interés.

Para la gestión efectiva de este conocimiento, se deberá desarrollar una base de datos centralizada que funcione como el eje principal para el registro y mantenimiento de todas las obligaciones de

cumplimiento. Esta herramienta no solo servirá para documentar, sino que también se diseñará para ser un recurso de fácil acceso y constante actualización, asegurando que la información refleje fielmente el entorno legal en vigor en todo momento.

En complemento a estas medidas, el Ministerio implementará una estrategia de comunicación efectiva, acompañada de programas de formación, con el fin de mantener a todos los/las funcionarios/as y partes interesadas debidamente informados sobre las obligaciones legales y contractuales que recaen sobre sus funciones específicas. Esto facilitará una cultura de seguridad informática compartida y la responsabilidad colectiva en la observancia del cumplimiento normativo, en consonancia con los controles A.18.01.01 de la ISO 27001.

Leyes Generales

- Ley Nº 20.478: Recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones.
- Ley Nº 20.285: Acceso a la información pública.
- Ley Nº 17.336: Propiedad intelectual.
- Ley Nº 19.927: Modifica códigos penales en materia de delitos de pornografía infantil.
- Ley Nº 19.799: Documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley Nº 18.845: Establece sistema de microcopia o micrograbación de documentos.
- Ley Nº 19.628: Protección de datos personales.
- Ley Nº 21.180: Transformación digital del estado.
- Ley Nº 21.459: Normas sobre delitos informáticos, adecuación al Convenio de Budapest.

Decretos y Reglamentos

- DFL N° 1-19.653, 2000: Texto refundido de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
- Decreto Nº 181, 2002: Reglamento de la Ley Nº 19.799 sobre documentos electrónicos y firma electrónica.
- Decreto Nº 1299, 2005: Normas sobre la red de conectividad del Estado.
- Decreto Nº 83, 2005: Norma técnica sobre seguridad y confidencialidad de documentos electrónicos.
- Decreto Nº 93, 2006: Norma técnica contra mensajes electrónicos masivos no solicitados.

- Decreto Nº 1, 2015: Norma técnica sobre sistemas y sitios web de la Administración del Estado.
- Decreto Nº 533, 2015: Creación de comité interministerial sobre ciberseguridad.

Instructivos y Políticas

- Instructivo Presidencial Nº 008, 2018: Medidas urgentes en materia de ciberseguridad.
- Instructivo Presidencial Nº 006, 2004: Implementación y uso de la firma electrónica.
- Instructivo Presidencial Nº 001, 2017: Implementación de la Política Nacional sobre Ciberseguridad.
- Política Nacional de Ciberseguridad, 2018.

Normas Técnicas y Circulares

- NCh-ISO 27001:2013: Sistema de gestión de seguridad de la información.
- NCh-ISO 27002:201: Tecnología de la información – Código de prácticas.
- Circular N° 51, 2009: Disposiciones sobre eliminación de documentos.
- Oficio circular N° 28.704, 1981: Disposiciones sobre eliminación de documentos.

Control A.18.01.03 Protección de los registros

El Área de Tecnología de la Información, deberá establecer y mantener un sistema de clasificación de registros. Este sistema discernirá el nivel de sensibilidad y relevancia de cada tipo de registro, determinando así el grado de protección y las normas de retención específicas que deben ser aplicadas. La importancia y la confidencialidad de la información marcarán las pautas para su resguardo y manejo.

Para el acceso y manejo de la información clasificada, se definirán claramente los perfiles de autorización, garantizando que sólo personal debidamente habilitado pueda interactuar con estos registros. Se estandarizarán y aplicarán procedimientos que regirán desde la generación hasta el almacenamiento, pasando por la transmisión y llegando a la destrucción de los registros, para asegurar un tratamiento adecuado en todas las etapas de su ciclo de vida.

Con respecto a la destrucción segura de la información, se adoptarán métodos que aseguren la imposibilidad de recuperar o reconstruir los datos. Esto incluirá la trituración de documentos en el caso de registros físicos y procesos como la purga y desmagnetización de soportes digitales

para los registros electrónicos. Estas prácticas buscan prevenir cualquier riesgo de divulgación o acceso no autorizado post destrucción, cumpliendo así con los más altos estándares de seguridad de la información.

Control A.18.02.01 Revisión independiente de la seguridad de la información

El Área de Tecnología de la Información se encargará de elaborar un plan detallado para la realización de auditorías internas y externas, con el propósito de revisar meticulosamente cada componente del sistema de gestión de seguridad de la información (SGSI). Este calendario contemplará una cobertura exhaustiva y se estructurará para garantizar una evaluación integral a lo largo del tiempo.

En cuanto a la selección de los auditores, se establecerán criterios estrictos para asegurar que estos profesionales sean completamente independientes y posean la competencia técnica requerida. Esto es fundamental para mantener la objetividad y confiabilidad de la evaluación de la seguridad de la información.

Finalmente, se definirá un procedimiento específico para el tratamiento de los hallazgos detectados durante las auditorías. Este proceso incluirá la identificación clara de las acciones correctivas, la asignación de responsables para su implementación y un sistema de seguimiento que permita monitorear el progreso en la resolución de cualquier debilidad o incumplimiento. Este enfoque proactivo y estructurado asegura que la gestión de los hallazgos de auditoría sea eficaz y conduzca a la mejora continua del SGSI.

Control A.18.02.02 Cumplimiento con las políticas y normas de seguridad

La estrategia del Área de Tecnologías de la Información para reforzar la adhesión a las políticas y normativas de seguridad incluirá un enfoque multidimensional.

Se dará prioridad a la concienciación y capacitación, desarrollando programas de formación regular y campañas de sensibilización que enfaticen la importancia de seguir las normas y políticas de seguridad. El objetivo es inculcar una cultura de seguridad entre los empleados y colaboradores, conscientes de su rol en la protección de la información.

En paralelo, se establecerá un proceso de gestión de incidentes. Este proceso incluirá protocolos para la notificación y la investigación de incidentes, así como procedimientos estructurados para la respuesta inmediata y el aprendizaje posterior a los eventos de seguridad, con el fin de evitar recurrencias.

Finalmente, se definirá un marco de aplicación para abordar el incumplimiento de las políticas. Este marco especificará las consecuencias, que podrían abarcar desde advertencias formales

hasta sanciones disciplinarias. Este régimen de consecuencias servirá como disuasivo efectivo y reafirmará el compromiso de la institución con la seguridad de la información.

Control A.18.02.03 Verificación del cumplimiento técnico

El Área de Tecnología de la Información deberá instruir un protocolo de evaluaciones y pruebas para confirmar periódicamente que la configuración técnica de los sistemas esté en concordancia con las políticas de seguridad. Este protocolo incluirá la realización de análisis de vulnerabilidades, pruebas de penetración y auditorías de seguridad de aplicaciones, que permitirán una detección proactiva de posibles falencias, contando con las mismas

Para ejecutar estas evaluaciones, se emplearán herramientas y técnicas avanzadas, combinando soluciones de software tanto automatizadas como manuales. Este enfoque mixto facilitará una verificación integral de las salvaguardas técnicas en uso, ofreciendo una perspectiva detallada de la postura de seguridad actual dentro de la institución.

Se deberá documentar como parte de la mejora continua de los procedimientos de seguridad. Cualquier anomalía o vulnerabilidad detectada se registrará meticulosamente, y se desarrollará un plan de acción correctivo. Este proceso iterativo es fundamental para fortalecer el cumplimiento técnico y evolucionar constantemente frente a las amenazas cambiantes y los avances tecnológicos.

8. Control

Elaborado por: Jorge Romero Vargas
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
Sebastián Aguirre Ulloa Asesor División Jurídico-Legislativa	Christian Valenzuela Lorca Jefe Gabinete de la Subsecretaria
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
Fecha: 10-11-2023