Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.07.02.01	Responsabilidades de la dirección
A.07.02.02	Concientización, educación y formación en seguridad de la información

Control de Versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
15-06-2016	1.0	Marcelo Aliaga Q. Liliana Reyes G.	Elaboración de Procedimiento
05-10-2016	1.1	Marcelo Aliaga Q. Liliana Reyes G.	Modificación de texto y configuración de documentos
06-10-2016	1.2	Marcelo Aliaga Q. Liliana Reyes G.	Modificación formato portada, tabla control de versiones, marcos de imágenes, Objetivo de control
30-11-2016	1.3	Vicente Manríquez	Modificación de texto
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"*
27-09-2018	3.0	Jorge Romero V. Solange Godoy C.	Se asocia a este documento control N° A.07.02.01, se agrega

			registro de operación
03-10-2023	3.1	Jorge Romero V.	Actualización sección firmantes. Mejora en el formato y redacción del documento. Complementa roles y responsabilidades. Mejora sección definiciones, plan anual de sensibilización y registros de operación. Incorpora lenguaje inclusivo en el documento.

1. Introducción

El Ministerio Secretaría General de la Presidencia dispone del presente documento, "Procedimiento de Sensibilización de Seguridad de la Información", 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.07.02.01

"La dirección debe solicitar a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización".

- Requisito de Control, A.07.02.01 NCh/ISO 27001:2013

Control A.07.02.02

"Todos los empleados de la organización, y en donde sea pertinente los contratistas, deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral".

- Requisito de Control, A.07.02.02 NCh/ISO 27001:2013

2. Objetivo

El objetivo de este procedimiento de sensibilización es establecer un marco estructurado para incrementar la conciencia sobre la seguridad en la gestión de la información dentro del Ministerio, asegurando que tanto funcionarios/as como colaboradores comprendan sus obligaciones en este ámbito. Se pretende inculcar una robusta cultura de seguridad de la información que impulse a los usuarios/as a ejercer sus funciones con responsabilidad y mayor protección. A través de un modelo, planificaremos, organizaremos y llevaremos a cabo actividades de sensibilización, orientando y formando a los miembros de la institución en las mejores prácticas de seguridad. Además, identificaremos y mitigaremos los riesgos asociados a dichas actividades para reforzar las futuras estrategias de prevención. Con un enfoque en la educación continua, buscaremos solidificar la postura de seguridad del Ministerio, fomentando la comprensión y aplicación de prácticas de seguridad que minimicen los riesgos de incidentes y que promuevan una respuesta adecuada ante eventuales vulnerabilidades o ataques. Este programa no solo propiciará una conciencia de seguridad integral entre los colaboradores, sino que también asegurará que las políticas y normativas vigentes se cumplan de manera consistente.

3. Alcance

El alcance de este procedimiento va dirigido a todo el personal con acceso a los sistemas y servicios de la institución. El programa incluye capacitaciones regulares y variadas, como formación en línea, talleres, simulacros y comunicaciones continuas, abarcando temas críticos desde la gestión de contraseñas hasta la prevención de phishing y la respuesta ante incidentes. Se implementarán evaluaciones para medir la eficacia del programa, con responsabilidades claramente asignadas al Encargado/a de Seguridad de la Información, al Encargado/a del área de Tecnologías de la Información, al Comité de Seguridad y a los usuarios/as, asegurando el cumplimiento y facilitando la revisión y mejora continua en función de la retroalimentación recibida y los cambios en el panorama de amenazas y regulaciones.

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 al Procedimiento de Sensibilidad de la Seguridad de la Información, asimismo, es responsabilidad de:

- **Encargado/a Área de Tecnologías de la Información**
  Respaldar la estrategia y ejecución del programa asegurándose de que la infraestructura tecnológica esté alineada con las necesidades educativas, proporcionar los recursos técnicos necesarios, coordinar con el equipo de Tecnologías de la Información para reforzar las políticas de seguridad, y actuar como un enlace comunicativo entre el Encargado/a de Seguridad de la Información y los diferentes centros de responsabilidad. Evaluar la tecnología en uso, asegurando que respalde los objetivos de sensibilización y contribuir al ciclo de mejora continua del programa.
- **Encargado/a de la Seguridad de la Información**
  Identificar las necesidades de capacitación de la organización, el desarrollo y la actualización de materiales educativos, la organización de sesiones de entrenamiento, y la medición de la efectividad del programa de sensibilización. Garantizar que las políticas y procedimientos de seguridad estén al día y en cumplimiento con las regulaciones pertinentes, promover una cultura de seguridad dentro de la institución, y gestionar los recursos asignados para la educación en seguridad de la información.

- **Comité de Seguridad de la Información**
  Establecer las políticas y estrategias que enmarcan la sensibilización, coordinar esfuerzos entre los distintos centros de responsabilidad, y evaluar la efectividad del programa, promoviendo una cultura institucional que prioriza la seguridad de la información.
- **Funcionarios/as o Colaboradores**
  Participar activamente en capacitaciones, adherirse a las políticas de seguridad, mantenerse vigilantes contra actividades sospechosas, reportar incidentes, actualizar continuamente sus conocimientos en seguridad y practicar comportamientos seguros. Contribuir a fomentar una cultura de seguridad consciente entre sus compañeros, actuando como defensores y ejemplificando buenas prácticas en su entorno laboral diario.

5. Definiciones

Sistema de Gestión de Seguridad de la Información (SGSI)
Marco sistemático que maneja proactivamente la protección de la información confidencial de la institución. Este sistema integral abarca a funcionarios/as y colaboradores, los procesos y la tecnología de la información mediante la aplicación de un proceso de gestión de riesgos continuo.

Control de acceso
Conjunto de procedimientos establecidos para asegurar que solo las personas autorizadas puedan acceder a la información y a los sistemas relevantes. Esto se logra mediante la implementación de controles tanto físicos como digitales.

Gestión de incidentes de seguridad de la información
Se refiere a los protocolos estandarizados requeridos para una gestión eficaz de los incidentes de seguridad, incluyendo su identificación, clasificación, respuesta inmediata y seguimiento detallado para fortalecer las estrategias de prevención.

Evaluación de riesgos
Este proceso esencial identifica, estima y prioriza los riesgos a la confidencialidad, integridad y disponibilidad de la información. Se basa en la valoración de la probabilidad de ocurrencia y su potencial impacto.

Tratamiento de riesgos

Tras la evaluación, se deben identificar, seleccionar y justificar las opciones para el tratamiento de riesgos, tales como su mitigación, transferencia o aceptación, seguidas de una documentación detallada.

Conciencia de seguridad

Representa el nivel de entendimiento y conocimiento de los individuos sobre las amenazas a la seguridad de la información y las acciones requeridas para mitigar dichas amenazas, incluido el reconocimiento de tácticas engañosas como el phishing, el vishing y el smishing.

Capacitación de seguridad

Se compone de actividades educativas planificadas que mejoran las habilidades de los funcionarios/as o colaboradores en seguridad de la información, desde cursos en línea hasta talleres y simulacros de incidentes.

Política de seguridad de la información

Documento formal que detalla las reglas y procedimientos que funcionarios/as, colaboradores y usuarios/as deben seguir para proteger la información de la institución.

Evaluación de vulnerabilidades

Es el proceso de identificar y cuantificar las debilidades de los sistemas, que puede incluir tanto el uso de herramientas automatizadas como revisiones manuales.

Respuesta a incidentes

Describe las acciones estructuradas y los procedimientos que se activan ante un incidente de seguridad para su pronta resolución y documentación con fines de aprendizaje y mejora.

Cumplimiento regulatorio

Implica asegurar la conformidad con leyes, regulaciones y directrices aplicables a la gestión de información en el contexto relevante.

Ciberseguridad

Es la disciplina que comprende la protección de sistemas, redes y datos contra accesos no autorizados o daños, y la prevención de interrupciones de servicio.

Gestión de activos de información
Proceso que asegura la identificación, clasificación y manejo adecuado de los activos de información a lo largo de su ciclo de vida.

Continuidad del negocio y recuperación ante desastres
Estrategias que permiten a la institución mantener y restaurar rápidamente sus operaciones después de incidentes graves.

Cultura de seguridad de la información
Se refiere al conjunto de valores y prácticas que determinan cómo una institución aborda la protección de su información.

Seguridad de la información
Conjunto de estrategias para salvaguardar la información frente a accesos, usos, divulgaciones y alteraciones no autorizadas.

Sensibilización
Se trata de las iniciativas educativas destinadas a informar a funcionarios/as y colaboradores de la institución, sobre las políticas de seguridad y fomentar comportamientos seguros.

Confidencialidad, integridad y disponibilidad
Principios fundamentales de la seguridad de la información, que buscan asegurar que la información solo sea accesible para autorizados, que se mantenga íntegra y que esté disponible cuando se necesite.

Riesgo de seguridad de la información
Es la posibilidad de que se materialice un daño o pérdida debido a vulnerabilidades o ataques a la seguridad de la información.

Gestión de riesgos
Es la identificación, análisis y mitigación continuos de los riesgos de seguridad, adaptándose al cambio constante del entorno institucional.

Incidente de seguridad
Eventos que ponen en riesgo la operatividad y la seguridad de la información de la institución.

Phishing y malware
Ataques que buscan engañar a las personas para obtener información confidencial o dañar sistemas, respectivamente.

Procedimiento
Instrucciones detalladas para ejecutar actividades de manera segura y eficaz.

Proveedores
Personas o entidades que interactúan con la información de la organización y que pueden ser internos o externos.

Violación de datos
Una brecha de seguridad que resulta en la exposición no autorizada de información sensible.

Cumplimiento
El acto de adherirse a leyes, regulaciones y políticas aplicables.

Control A.07.01.01

Elaboración de políticas claras y accesibles
Redactar políticas de seguridad de la información claras, concisas y fácilmente accesibles. Se deberá asegurar que las políticas cubran todos los aspectos relevantes de la seguridad de la información y sean aprobadas por autoridades.

Comunicación y difusión
Difundir las políticas y procedimientos a través de múltiples canales, como correo electrónico, intranet y reuniones. Incluir la seguridad de la información en la orientación de nuevos funcionarios/as, colaboradores y en los contratos con proveedores.

Programas de concienciación y formación
Desarrollar y mantener un programa de formación en seguridad de la información que sea obligatorio para todos. Personalizar la formación según los diferentes roles y niveles de acceso a la información. Incluir ejemplos prácticos y consecuencias del incumplimiento en las sesiones de capacitación.

Acuerdos de confidencialidad y compromiso
Solicitar la firma de acuerdos de confidencialidad y compromisos de seguridad de la información. Asegurar que funcionarios, colaboradores y proveedores de servicios para la institución entiendan las expectativas y las consecuencias del incumplimiento.

Integración en procesos y procedimientos
Integrar los requisitos de seguridad de la información en los procesos operativos diarios. Desarrollar procedimientos específicos para tareas críticas relacionadas con la seguridad de la información.

Evaluación periódica de conformidad
Realizar auditorías y revisiones regulares para verificar el cumplimiento de las políticas de seguridad. Proporcionar retroalimentación y realizar seguimiento para asegurar la mejora continua.

Mecanismos de reporte
Establecer canales claros para que los funcionarios/as, colaboradores y proveedores de servicios de la institución informen de incidentes de seguridad o vulnerabilidades. Garantizar que el proceso de reporte sea simple y que proteja al informante.

Gestión de incidentes y mejora continua
Tener un proceso establecido para responder a los incidentes de seguridad. Utilizar los incidentes y las brechas de seguridad como oportunidades de aprendizaje para mejorar las políticas y formaciones.

Sanciones y consecuencias
Definir y comunicar las consecuencias de no cumplir con las políticas de seguridad de la información. Aplicar las sanciones de manera justa y consistente para reforzar la importancia del cumplimiento.

Revisión y actualización de políticas
Revisar y actualizar periódicamente las políticas de seguridad de la información para reflejar los cambios en el entorno y en la institución.

Liderazgo visible
Las autoridades deben mostrar un compromiso visible con la seguridad de la información y actuar como modelo a seguir.

Reconocimiento y recompensa
Implementar un sistema de reconocimiento para los funcionarios/as y colaboradores que promueven activamente y apoyan las prácticas de seguridad de la información.

Control A.07.02.02

Evaluación de necesidades de formación
Se deberá realizar una evaluación inicial de las necesidades de formación para identificar los conocimientos específicos en seguridad de la información que los funcionarios/as, colaboradores y contratistas deben poseer, basándose en sus roles y responsabilidades.

Desarrollo de contenidos de concientización
Se deberá crear o adquirir materiales de formación y concientización que sean relevantes para las políticas y procedimientos de seguridad de la organización. Estos materiales deben ser diseñados para ser atractivos y comprensibles para todos los niveles de la organización.

Programa de inducción para nuevos ingresos
Incluir una sesión de concientización en seguridad de la información como parte del programa de inducción de todos los nuevos funcionarios/as, colaboradores y proveedores, asegurando que comprendan las expectativas desde el comienzo de su relación laboral con la institución.

Capacitación continua y actualizaciones
Implementar un programa de formación continua que incluya actualizaciones regulares conforme a las políticas y procedimientos cambien o se actualicen, así como las leyes y regulaciones pertinentes. La frecuencia de estas actualizaciones debe ser determinada por los cambios en el entorno de amenazas, los incidentes de seguridad ocurridos y las leyes/regulaciones aplicables.

Metodologías de entrega
Utilizar diversas metodologías para entregar la formación y las actualizaciones, tales como e-learning, seminarios web, talleres presenciales y boletines informativos. Esto ayudará a mantener el interés y acomodar diferentes estilos de aprendizaje.

Verificación y seguimiento
Establecer mecanismos para verificar la asistencia y el entendimiento de la formación proporcionada. Esto puede incluir pruebas, encuestas y evaluaciones que deben ser completadas por los funcionarios/as colaboradores y proveedores para demostrar su comprensión.

Refuerzo y sensibilización continua
Mantener un programa de refuerzo que incluya carteles, recordatorios por correo electrónico y campañas de concientización para mantener la seguridad de la información visible y relevante en la vida cotidiana de los funcionarios/as y colaboradores.

Registro y documentación
Mantener registros documentados de todas las actividades de formación y concientización realizadas, incluidos los asistentes, los resultados de las evaluaciones y los comentarios para auditorías futuras y evaluaciones de eficacia del programa.

Revisión y mejora del programa
Realizar revisiones periódicas del programa de concientización y formación para evaluar su eficacia y hacer mejoras. Esto puede basarse en los comentarios de los funcionarios/as y colaboradores, las observaciones de los cambios de comportamiento o las tendencias identificadas en los incidentes de seguridad.

Comunicación de las Autoridades
Asegurar el apoyo y la comunicación de las Autoridades respecto a la importancia de la formación y concientización en seguridad de la información, lo que refuerza la cultura de seguridad en toda la institución.

Programa Anual de Sensibilización

Planificación	Actividades
Enero	Sensibilización en Seguridad de la Información • Lanzamiento oficial con mensaje de las autoridades. • Presentación de las iniciativas de seguridad de información planificadas para el año.
Febrero	Concienciación sobre Phishing y temas relacionados • Talleres interactivos de reconocimiento de correos electrónicos y comunicaciones fraudulentas. • Simulaciones de phishing para evaluar la susceptibilidad y reforzar las prácticas de detección.
Marzo	Gestión Segura de Contraseñas • Sesiones educativas sobre la importancia de las contraseñas fuertes y el uso de gestores de contraseñas. • Campaña para actualizar las contraseñas y adoptar autenticación multifactor.
Abril	Seguridad en Redes Sociales y Online • Formación sobre los riesgos asociados con las redes sociales y

	la exposición de información personal. • Evaluaciones interactivas de perfiles en redes sociales para identificar riesgos potenciales.
Mayo	<u>Protección contra Malware y Ransomware</u> • Distribución de materiales educativos sobre cómo evitar malware. • Pruebas de conocimiento con recompensas para quienes identifiquen correctamente los signos de advertencia de malware.
Junio	<u>Seguridad Física y de la Información</u> • Actividades centradas en la seguridad física, como el manejo adecuado de documentos confidenciales y la protección de dispositivos móviles. • Ejercicios de evacuación y protección de la información sensible en casos de emergencia física.
Julio	<u>Buenas Prácticas en el Escritorio y en el Lugar de Trabajo</u> • Campaña visual en las oficinas con recordatorios sobre bloqueo de pantalla, gestión de visitantes y limpieza de escritorio. • Auditorías sorpresa de seguridad en el lugar de trabajo.
Agosto	<u>Seguridad en la Nube y en el Teletrabajo</u> • Webinars sobre seguridad y mejores prácticas al trabajar de forma remota. • Checklist de autoevaluación para el entorno de trabajo en casa.
Septiembre	<u>Reconocimiento de Ingeniería Social</u> • Juegos de rol y simulaciones para enseñar a los funcionarios/as y colaboradores a manejar intentos de ingeniería social. • Competencias de reconocimiento de tácticas de ingeniería social con premios.

Octubre	<u>Mes de la Concienciación Nacional de Ciberseguridad</u> • Participación en eventos y actividades externos. • Concursos de ensayos o proyectos relacionados con la seguridad de la información.
Noviembre	<u>Gestión de Incidentes y Planes de Respuesta</u> • Simulacros de incidentes de seguridad para practicar la respuesta y recuperación. • Talleres de revisión de políticas de respuesta a incidentes.
Diciembre	<u>Revisión y Reflexión</u> • Encuestas para obtener retroalimentación sobre el programa de sensibilización. • Sesión de cierre para discutir aprendizajes y reconocer contribuciones sobresalientes.
Durante el periodo	• Boletines mensuales sobre temas de seguridad de la información. • Reconocimientos y recompensas para comportamientos seguros destacados. • Paneles de discusión para abordar dudas y situaciones de la vida real. • Actualizaciones constantes de contenido en la intranet y recordatorios a través de correos electrónicos y carteles.

6. Registro de Operación

Planificación y Lanzamiento

- Minutas de las reuniones de planificación del programa.
- Documento del programa anual de sensibilización con objetivos y calendario.
- Comunicados de lanzamiento y mensajes de autoridades.

Formación y Educación

- Listas de asistencia a las sesiones de capacitación y talleres.
- Registros de acceso y completamiento de cursos en línea.
- Evaluaciones y pruebas de conocimiento previas y posteriores a las capacitaciones.
- Registros de simulaciones de phishing y resultados.

Campañas y Actividades

- Documentos de campañas específicas
- Fotos o grabaciones de eventos y actividades de sensibilización (con el debido consentimiento).
- Registros de participación en concursos y ganadores.

Evaluación y Mejora Continua

- Resultados de las auditorías de seguridad en el lugar de trabajo.
- Resultados de las evaluaciones de vulnerabilidad.
- Informes de seguimiento y revisión de incidentes simulados.

Comunicaciones

- Copias de los boletines mensuales y otros materiales de comunicación distribuidos.
- Registros de actualizaciones realizadas en la intranet o el sistema de gestión de aprendizaje.
- Registros de paneles de discusión, incluyendo preguntas y respuestas frecuentes.

Retroalimentación y Encuestas

- Resultados de encuestas de satisfacción y retroalimentación de los/las funcionarios/as y colaboradores.
- Informes de análisis de retroalimentación y acciones tomadas en respuesta.

Involucramiento de autoridades y centros de responsabilidad

- Documentación sobre la participación de autoridades en el programa.
- Registros de las colaboraciones de centros de responsabilidad y las reuniones de coordinación.

Cumplimiento y evidencia de acciones correctivas

- Documentación de las medidas tomadas para cerrar cualquier brecha identificada en la seguridad de la información.
- Informes de cumplimiento y auditoría interna o externa relacionados con la sensibilización en seguridad de la información.

Gestión de Incidentes

- Informes detallados de incidentes de seguridad, lo cuales podrán ser reales o simulados, incluyendo respuestas y lecciones aprendidas.

Infraestructura de Seguridad de la Información

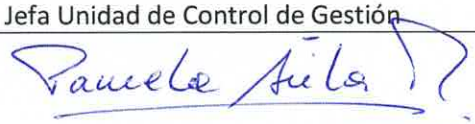
- Documentos que demuestren la actualización y mantenimiento de las herramientas y sistemas de seguridad.

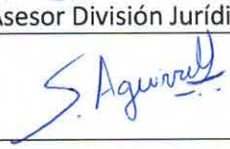
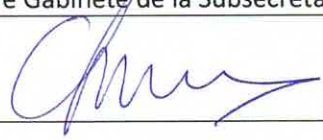
7. Control

Elaborado por: Jorge Romero Vargas

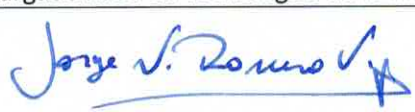
Fecha: 10-11-2023

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