Controles NCH ISO 27001:2013 Relacionados

CONTROL	NOMBRE
A.17.01.01	Planificación de la continuidad de la seguridad de la información
A.17.01.02	Implementación de la continuidad de la seguridad de la información
A.17.01.03	Verificación, revisión y evaluación de la continuidad de la seguridad de la información

CONTROL DE VERSIONES

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
01-07-2019	1.0	Jorge Romero V. Solange Godoy C.	Elaboración documento
10-11-2023	1.1	Jorge Romero	Actualización 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.

1. Introducción

El Ministerio Secretaría General de la Presidencia dispone del presente documento, "Política de la Continuidad de la 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.17.01.01 Planificación de la continuidad de la seguridad de la información

"La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre".

- Requisito control A.17.01.01 NCH ISO 27001-2013

Control A.17.01.02 Implementación de la continuidad de la seguridad de la información

"La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa".

- Requisito control A.17.01.02 NCH ISO 27001-2013

Control A.17.01.03 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

"La organización debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas".

- Requisito control A.17.01.03 NCH ISO 27001-2013

2. Alcance

La política de continuidad de la seguridad de la información tiene un alcance integral, abarcando todos los aspectos críticos como los datos y sistemas de información, los procesos de la institución, los/las funcionarios/as, colaboradores, las instalaciones físicas, y las relaciones con proveedores y terceros. Incluye el cumplimiento de requisitos legales y normativos, y se extiende a la gestión de riesgos, planificación de emergencias, comunicaciones, así como a los procedimientos de recuperación y restauración. Este enfoque holístico asegura que todos los componentes esenciales de la institución estén preparados y protegidos contra interrupciones, garantizando la continuidad operativa y la seguridad de la información en diversas circunstancias.

3. Objetivo

La política de continuidad de la seguridad de la información tiene como objetivo asegurar que las operaciones críticas y los datos de la institución permanezcan seguros y accesibles en caso de interrupciones. Centrada en la protección de los activos de información y la minimización del impacto de cualquier evento disruptivo, esta política establece procedimientos para una recuperación rápida y eficiente, garantiza el mantenimiento de operaciones esenciales, y cumple con las normativas legales y de gestión de riesgos. Además, promueve la concienciación y

capacitación de funcionarios/as y colaboradores, siendo un componente vital para la resiliencia institucional ante situaciones adversas.

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 Continuidad de la Seguridad de la Información, asimismo, es responsabilidad de:

- **Encargado/a Área de Tecnologías de la Información**

  Asegurar que la infraestructura tecnológica respalde los planes de continuidad y recuperación. Coordina la integración de sistemas y procesos de negocio para garantizar la continuidad operativa y la rápida restauración en caso de interrupciones. Gestionar los recursos tecnológicos necesarios, adopción de nuevas tecnologías para mejorar la capacidad de recuperación y resiliencia de la institución. Su papel es vital para mantener la operatividad y eficiencia tecnológica durante situaciones adversas.

- **Encargado/a de la Seguridad de la Información**

  Desarrollo e implementación de la política, centrándose en la seguridad de los datos. Responsable de la evaluación de riesgos, identificar y mitigar amenazas a la seguridad de la información. Desarrollo y mantención del plan de recuperación de desastres, asegurando la protección y recuperación de la información. Realizar pruebas regulares para garantizar la efectividad de estos planes y promover la capacitación y concienciación sobre seguridad entre los/las funcionarios/funcionarias y colaboradores, siendo un pilar clave en la resiliencia de la institución frente a incidentes de seguridad.

- **Comité de Seguridad de la Información**

  Desarrollo, revisión y supervisión de esta política. Coordinar la colaboración entre centros de responsabilidad para integrar diversas perspectivas en la planificación de la continuidad, evalúa riesgos, establece procedimientos y protocolos de recuperación, y supervisa la implementación y las pruebas de los planes. Además, fomenta la formación y concienciación entre los/las funcionarios/as y colaboradores, gestiona la respuesta a incidentes y emergencias, y mantiene una comunicación fluida con autoridades. Su enfoque en la revisión y mejora continua asegura que la política se mantenga efectiva y alineada con los cambios en el entorno tecnológico y lineamiento institucional

5. Mecanismo de difusión

Es responsabilidad del Comité de Seguridad de la Información, la difusión de esta política, el que se enviará por correo electrónico y deberá permanecer a disposición de todos los trabajadores de este Ministerio en la Intranet institucional.

6. Evaluación y revisión

El tiempo de evaluación y revisión estándar de esta Política, será en un plazo máximo de 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

A.17.01.01 Planificación de la continuidad de la seguridad de la información

Se deberá establecer, mantener y revisar continuamente un plan documentado para asegurar la continuidad de la seguridad de la información ante interrupciones en las operaciones de la institución. Se buscará garantizar responder de manera eficiente y efectiva a incidentes o desastres que puedan comprometer la integridad, disponibilidad y confidencialidad de la información crítica. La planificación de la continuidad involucra la identificación de amenazas potenciales, la evaluación de impactos en el negocio, y el desarrollo de estrategias y procedimientos que permitan mantener o restaurar rápidamente las operaciones de TI y la seguridad de la información en caso de una interrupción. Este enfoque proactivo tiene como finalidad minimizar el impacto en las operaciones comerciales, proteger los intereses de las partes interesadas y cumplir con los requisitos legales y normativos correspondientes.

Impacto en el Negocio (BIA)
Llevar a cabo un análisis de impacto en el negocio regularmente para identificar y evaluar los efectos de posibles interrupciones en las operaciones críticas y la seguridad de la información. Se deberán establecer prioridades de recuperación basadas en este análisis.

Gestión de Riesgos
Identificar y evaluar riesgos que puedan afectar la seguridad de la información. Se deberán implementar estrategias adecuadas para mitigar estos riesgos.

Mitigación de Riesgos
Desarrollar e implementar medidas preventivas para reducir la probabilidad y el impacto de interrupciones en la seguridad de la información.

Pruebas de Continuidad
Realizar pruebas regulares de los planes de continuidad y recuperación de desastres para asegurar su efectividad y actualizarlos según sea necesario.

Gestión de Incidentes de Seguridad
Establecer y mantener un proceso efectivo para la gestión de incidentes de seguridad, garantizando una respuesta rápida y adecuada a los eventos que comprometan la información.

Estrategias de Recuperación
Desarrollar y mantener planes de acción específicos para restaurar las operaciones de TI y la seguridad de la información después de una interrupción.

A.17.01.02 Implementación de la continuidad de la seguridad de la información
Asegurar la implementación efectiva y operativa de las estrategias y procedimientos de continuidad de la seguridad de la información dentro de la institución. Se deberá mantener un enfoque en poner en práctica los planes de continuidad desarrollados, garantizando que las medidas, recursos y capacidades necesarias estén disponibles y sean funcionales para responder ante interrupciones. Incorporar la asignación de responsabilidades, la formación y concienciación del personal, y la realización de pruebas y ejercicios periódicos para verificar la eficacia de los planes de continuidad. El propósito es asegurar que la institución esté preparada para mantener o restaurar rápidamente sus operaciones de información crítica en el caso de una interrupción, minimizando así el impacto en las operaciones del negocio, protegiendo la información vital.

Continuidad de la Seguridad de la Información
Establecer y mantener un conjunto robusto de procesos y medidas para asegurar la operatividad y protección de la información y los sistemas de información.

Activación del Plan de Continuidad
Definir criterios claros para determinar cuándo y cómo se debe implementar el PCSI, garantizando una respuesta oportuna y adecuada ante incidentes.

Roles y Responsabilidades en Continuidad
Asignar roles y responsabilidades específicas a individuos o equipos para la gestión efectiva de la continuidad de la seguridad de la información.

Recursos para la Continuidad
Asegurar la disponibilidad de todos los recursos necesarios, incluyendo personal, tecnología, información y financiamiento, para implementar eficazmente el PCSI.

Procedimientos de Respuesta a Incidentes
Establecer y mantener procedimientos detallados para responder de manera eficiente a incidentes de seguridad que afecten la continuidad.

Comunicaciones de Emergencia
Desarrollar y probar canales de comunicación interna y externa para asegurar una comunicación eficiente durante y después de un incidente o interrupción.

Entrenamiento y Simulacros de Continuidad
Realizar actividades regulares de formación y práctica para preparar al personal en la implementación del PCSI y validar la efectividad de los procedimientos de continuidad.

Coordinación con Terceros
Establecer procesos de colaboración con proveedores y otras entidades externas para asegurar la integración y coherencia de los planes de continuidad.

Revisión Post-incidente
Llevar a cabo análisis post-incidente para evaluar la gestión del incidente y determinar áreas de mejora en los procedimientos y planes de continuidad.

Actualización del PCSI
Realizar revisiones periódicas y actualizaciones del PCSI para reflejar cambios en el entorno operativo, tecnológico y de riesgos, incorporando lecciones aprendidas.

Criterios comunes de activación

Violaciones significativas de la seguridad
Activar el PCSI en caso de ataques cibernéticos graves como ransomware, intrusiones que comprometan datos sensibles, o cualquier otra violación que afecte la integridad, confidencialidad o disponibilidad de los datos críticos.

Fallo de infraestructura crítica
En caso de fallo de sistemas de TI esenciales, como servidores de datos, redes de comunicaciones o sistemas de almacenamiento, que impidan el acceso normal a la información.

Desastres naturales o ambientales
Situaciones como incendios, inundaciones, terremotos o cualquier otro desastre natural que impacte las operaciones físicas o tecnológicas de la institución.

Errores humanos o fallos técnicos
Errores significativos cometidos por empleados, o fallos técnicos que resulten en la pérdida o compromiso de información importante.

Interrupciones en el suministro de energía o servicios
Cortes de energía, interrupciones en los servicios de internet o telecomunicaciones que afecten críticamente las operaciones de la institución.

Compromiso de Acceso Físico o Lógico
Situaciones donde el acceso físico a las instalaciones críticas o el acceso lógico a los sistemas de información está comprometido o restringido de manera significativa.

Incumplimiento de Umbrales Predeterminados
Incumplimientos de umbrales predeterminados, como tiempos de inactividad o niveles de rendimiento, que indiquen una degradación crítica de los servicios de TI.

Alertas de Autoridades o Entidades Externas
Advertencias de autoridades gubernamentales, reguladores o socios tecnológicos sobre amenazas inminentes o incidentes en curso que puedan afectar la seguridad de la información.

Requisitos Legales o Regulatorios
Situaciones en las que los requisitos legales o regulatorios obligan a la implementación de medidas de continuidad para proteger datos sensibles o críticos.

A.17.01.03 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Se deberá asegurar la realización periódica de actividades de verificación, revisión y evaluación para mantener la eficacia y relevancia del Plan de Continuidad de la Seguridad de la Información (PCSI). Evaluar sistemáticamente si las estrategias y procedimientos de continuidad siguen siendo adecuados frente a los cambios en el entorno de la institución, las amenazas emergentes y los avances tecnológicos. Deberá incluir la revisión de los resultados de las pruebas y simulacros de continuidad, el análisis de incidentes recientes y la evaluación del desempeño del PCSI en situaciones reales. El propósito es identificar áreas de mejora, actualizar los planes según sea necesario y garantizar que la institución esté preparada para responder de manera efectiva a interrupciones futuras, protegiendo así la integridad, disponibilidad y confidencialidad de la información crítica.

Verificación de la continuidad

Implementar un proceso de comprobación regular para asegurar que todos los elementos del PCSI estén presentes, actualizados y sean funcionales.

Revisión de la continuidad

Realizar evaluaciones periódicas del PCSI para determinar su adecuación y efectividad, adaptándolo a las necesidades cambiantes de la institución.

Evaluación de la continuidad

Llevar a cabo análisis detallados del PCSI para medir su efectividad en situaciones reales o simuladas, identificando áreas de mejora.

Pruebas y simulacros

Desarrollar y ejecutar regularmente actividades prácticas y simulaciones de incidentes para validar la efectividad del PCSI.

Auditoría interna/externa

Facilitar revisiones independientes, tanto internas como externas, del PCSI para evaluar su conformidad con las políticas y procedimientos establecidos.

Mejora continua

Establecer un proceso para realizar ajustes y mejoras en el PCSI, basándose en los resultados de las pruebas, revisiones, evaluaciones y auditorías.

Retroalimentación de las partes interesadas

Recoger y analizar las opiniones y observaciones de empleados, colaboradores, proveedores y otros grupos relevantes para mejorar continuamente el PCSI.

Documentación del PCSI

Mantener una documentación detallada y actualizada de todas las políticas, procedimientos, pruebas, revisiones, evaluaciones y cambios realizados en el PCSI.

Reporte a las autoridades

Establecer un proceso para informar regularmente a las autoridades competentes sobre el estado y la efectividad del PCSI, incluyendo recomendaciones para mejoras.

Otras definiciones

- Plan de Continuidad del Negocio (BCP)
  El BCP es una estrategia integral destinada a asegurar la continuidad de las operaciones críticas de un negocio durante y después de una interrupción significativa. Cubre todos los aspectos del negocio, como procesos, personal, instalaciones y proveedores. Su objetivo principal es minimizar el impacto negativo en las operaciones comerciales y garantizar que las funciones vitales puedan continuar o reanudarse rápidamente en caso de una crisis, como desastres naturales, ataques cibernéticos o fallos técnicos.

- Plan de Recuperación de Desastres (DRP)
  El DRP se enfoca específicamente en la recuperación de sistemas y operaciones de tecnología de la información tras un desastre o interrupción grave. Se centra en la infraestructura tecnológica, incluyendo servidores, redes, bases de datos y sistemas de almacenamiento. El objetivo del DRP es restaurar rápidamente las capacidades de TI y los datos críticos para

minimizar el tiempo de inactividad y el impacto en las operaciones del negocio, asegurando que los sistemas tecnológicos esenciales vuelvan a estar en línea lo antes posible.

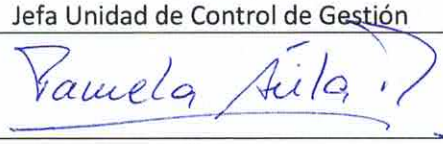
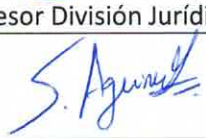
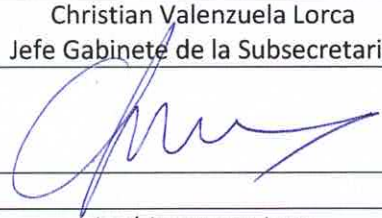
- Plan de Continuidad de la Seguridad de la Información (PCSI)
  El PCSI se centra en proteger y mantener la integridad, confidencialidad y disponibilidad de la información de la institución durante y después de una interrupción o incidente. Este plan aborda específicamente la seguridad de los datos, estableciendo protocolos para prevenir, responder y recuperarse de incidentes que amenacen la seguridad de la información. Su objetivo es garantizar que la información crítica se mantenga segura y accesible, incluso en situaciones adversas, minimizando así el riesgo de pérdida o compromiso de datos importantes.

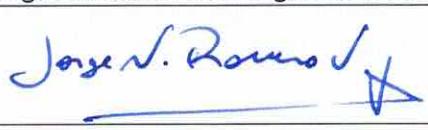
8. Control

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