SERVICIO NACIONAL DE CAPACITACIÓN PARA LA INDUSTRIA DE LA CONSTRUCCIÓN

DIRECTIVA DE SEGURIDAD DE LA INFORMACIÓN DEL SENCICO

RESOLUCIÓN Nº 000222-2024-02.00/SENCICO

Departamento de Informática

DICIEMBRE 2024

Firmado digitalmente por VASQUEZ ESPINOZA Luis Alberto FAU 20131377810 soft
Motivo: Doy V° B°
Fecha: 17.12.2024 10:47:13 -05:00

Firmado digitalmente por:
LAPA LOAYZA Luis Angel
FAU 20131377810 soft
Motivo: Doy V° B°
Fecha: 17/12/2024 10:25:46-0500

SENCICO	**DIRECTIVA**		**DI/PE/OAF-INF/N°003-2024**	
	TITULO: SEGURIDAD DE LA INFORMACIÓN DEL SENCICO			
	Aprobado por:	Presidencia Ejecutiva	Fecha de Aprobación:	
	Propuesto por:	Departamento de Informática		
	Deja sin Efecto:		Fecha de Publicación:	

1. OBJETIVO

Establecer un marco que asegure la protección de la información del SENCICO, preservando su confidencialidad, integridad y disponibilidad, mitigando los riesgos de seguridad de la información y cumpliendo con los requisitos legales.

2. ALCANCE

Las disposiciones contenidas en la presente directiva son de cumplimiento obligatorio de todas las unidades de organización del SENCICO.

3. VIGENCIA

Esta directiva entra en vigencia a partir de la emisión de la Resolución que aprueba la misma y su actualización se realiza en función a los cambios o necesidades futuras.

4. BASE LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y su modificatoria y su Reglamento aprobado por Decreto Supremo N° 030-2002-PCM,
- Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento aprobado por Decreto Supremo Nº 003-2013-JUS,
- Ley N° 28716, Ley de Control Interno de las entidades del Estado.
- Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y su Reglamento aprobado por Decreto Supremo Nº 029-2021-PCM
- Decreto Supremo N° 050-2018-PCM. Decreto que establece la definición de Seguridad Digital de ámbito nacional.
- Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información.

Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD.
- Resolución de Presidencia Ejecutiva N° 134-2018-02.00. Conformación del Comité de Gobierno Digital del SENCICO y modificatorias
- Resolución de Presidencia Ejecutiva N° 82-2021-02.00. Designación del Oficial de Seguridad Digital del SENCICO y modificatorias.

5. DEFINICIONES

5.1. Accesos: Permisos específicos que se le otorga al colaborador.

5.2. Acuerdos de niveles de servicio (ANS): Documentos que establecen las características y estándares de calidad del servicio adquirido, incluyendo aspectos relacionados con la seguridad de la información.

5.3. Activo: Activo de información relevante e instalaciones de procesamiento de información relevante.

5.4. Activo de información relevante: Conocimientos, datos y recursos que tienen valor para el SENCICO, viene a ser lo que una entidad valora y por lo tanto debe proteger, estos pueden ser: los datos no públicos creados o utilizados por un proceso, recursos o documentación (digital, papel u otro medio).

5.5. Áreas seguras: Ambientes donde se procesa, almacena o transmite información no pública, tales como: Data Centers, instalaciones del archivo, gabinetes de redes y comunicaciones, servicio de nube, entre otros.

5.6. Aspectos relevantes para el SGSI: Aspectos externos (sociales, políticos, normativos, financieros, tecnológicos, etc.) e internos (cultura organizacional, política, visión, misión, objetivos, acciones estratégicas, gobernanza, estructura orgánica, roles y responsabilidades, normativa interna, tecnologías de la información, etc.) que de alguna manera afectan la seguridad de la información y cómo se puede gestionar la seguridad de la información, y que son relevantes para el propósito del SENCICO.

5.7. Atención de incidentes de seguridad de la información: Procedimiento para identificar, evaluar y responder a los incidentes de seguridad de la información, con el objetivo de minimizar su impacto y restaurar la normalidad lo más rápido posible.

5.8. Auditoría: Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar el grado en que se cumplen los criterios de auditoría.

5.9. Auditoría a servicio: Proceso sistemático, independiente y documentado, aplicado a un servicio de contratista, para obtener evidencia de auditoría y evaluarla objetivamente para determinar el grado en que se cumplen los criterios de auditoría que, para este caso, son las cláusulas contractuales de seguridad de la información.

5.10. Carpeta de trabajo: Es una carpeta ubicado en la unidad C: del disco duro del equipo de cómputo (proporcionado por el SENCICO o de su propiedad debidamente autorizado para su uso en la red del SENCICO) que utiliza un usuario, en la cual deberá almacenar sus archivos de trabajo.

5.11. Clasificación de la información: Proceso de categorización de la información según su nivel de confidencialidad, integridad y disponibilidad, para determinar los controles de seguridad adecuados.

5.12. Colaborador: Miembro del personal interno del SENCICO que desempeña funciones y responsabilidades dentro de la entidad. Los colaboradores son considerados usuarios y tienen la responsabilidad de cumplir con las políticas y procedimientos de seguridad de la información, así como, proteger los activos de información y contribuir a la cultura de seguridad en la organización.

5.13. Comunicación relevante al SGSI: Es la comunicación entre las partes interesadas internas del SENCICO o entre el SENCICO y las partes interesadas externas sobre los componentes más relevantes del SGSI como son: a) la política, directivas y objetivos del SGSI, b) roles y responsabilidades de seguridad de la información, c) los procedimientos del SGSI, d) los cambios en el SGSI, e) los riesgos y oportunidades de seguridad de la información, f) incidentes o crisis de seguridad de la información, g) requisitos para los contratistas y h) entre otros.

5.14. Contratista: El proveedor que celebra un contrato con el SENCICO.

5.15. Criterios de auditoría: Conjunto de políticas, procedimientos o requisitos utilizados como referencia frente a la cual se compara la evidencia de la auditoría.

5.16. Debilidad de seguridad de la información: Vulnerabilidad o ausencia de control de seguridad de la información en un activo de información que puede ser explotada por una o más amenazas.

5.17. Dispositivo móvil: Equipo portátil como teléfonos móviles, tabletas y laptops de propiedad del SENCICO, utilizados por los colaboradores para acceder y procesar información.

5.18. Equipo de cómputo: Equipo electrónico que recibe y procesa datos para convertirlo en información y ejecutan tareas diversas. Posee una unidad central

de procesamiento, memoria principal, almacenamiento y algún dispositivo periférico. Pueden ser de escritorio o dispositivo móvil.

5.19. Equipo de cómputo desatendido: Equipo de cómputo que están funcionando sin presencia de su usuario.

5.20. Espacios de teletrabajo: Áreas o lugares donde los colaboradores realizan sus actividades laborales de forma remota, utilizando dispositivos y conexiones a internet.

5.21. Evento de seguridad de la información: Ocurrencia identificada de un sistema, servicio o red que indica una posible ruptura de la seguridad, de la política o una falla en los controles de seguridad, o una situación desconocida previamente que pueda ser relevante para la seguridad.

5.22. Evidencia de auditoría: Registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables.

5.23. Incidente de seguridad de la información: Uno solo o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la institución y amenazar la seguridad de la información.

5.24. Información no pública: Información contemplada expresamente en las excepciones establecidas en el Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, Ley N° 27806 (TUO de la Ley): información secreta, información reservada e información confidencial.

5.25. Manejo de activos: Conjunto de acciones y procedimientos para gestionar y proteger los activos de información de la organización, incluyendo su entrega, uso y devolución.

5.26. Medios removibles: Dispositivos capaces de recibir información y retenerla durante un periodo de tiempo, permitiendo su recuperación y empleo cuando sea necesario. Estos pueden ser: discos duros externos, cintas magnéticas, medios ópticos (CD-ROM, CD-RW, DVD, Blu-ray, entre otros) y memorias (USB, SD, SDHC, entre otras).

5.27. Partes interesadas relevantes al SGSI: Personas u organizaciones que pueden afectar, ser afectados por o percibirse a sí mismos como afectados por una decisión o actividad del SENCICO respecto al SGSI. Las partes interesadas pueden encontrarse tanto dentro (Consejo Directivo Nacional, Presidencia Ejecutiva, Gerencias, colaboradores, practicantes, entre otras) como fuera (PCM, CGR, MINJUSDH, ANSC, contratistas, alumnos, entre otras)

del SENCICO y pueden tener necesidades, expectativas y requisitos específicos para la seguridad de la información del SENCICO.

5.28. Propiedad intelectual: Derechos legales que protegen las creaciones originales de una persona o entidad, como invenciones, obras literarias, diseños, marcas registradas, entre otros.

5.29. Protección de datos personales: Conjunto de medidas y controles destinados a garantizar la privacidad y seguridad de la información personal de los individuos, de acuerdo con las leyes y regulaciones aplicables.

5.30. Proveedor: Persona natural o jurídica que vende o arrienda bienes, y/o presta servicios.

5.31. Requisitos de seguridad de la información: Conjunto de medidas y controles que deben cumplir los contratistas para garantizar la protección de la información y mitigar los riesgos asociados.

5.32. Riesgo: Efecto de la incertidumbre, posibilidad de ocurrencia de un evento adverso que afecte negativamente el logro de los objetivos del SGSI.

5.33. Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, por medio de un conjunto de medidas técnicas, organizativas y legales.

5.34. Sistema de Gestión de Seguridad de la Información (SGSI): Sistema integral que permite a las organizaciones gestionar de manera efectiva la seguridad de la información, protegiendo los activos y recursos relacionados a través de políticas, procedimientos y controles adecuados.

5.35. Trabajo a distancia: Teletrabajo o trabajo remoto.

5.36. Trabajo remoto: Prestación de servicios subordinada con la presencia física del trabajador en su domicilio o lugar de aislamiento domiciliario, utilizando cualquier medio o mecanismo que posibilite realizar las labores fuera del SENCICO, siempre que la naturaleza de las labores lo permita.

5.37. Transferencia de medios físicos: Proceso de envío o transporte de dispositivos o soportes físicos que contienen información, asegurando su protección e integridad durante el traslado.

5.38. Usuario: Se refiere a cualquier persona que utiliza los activos de información y los servicios proporcionados por el SENCICO, ya sea colaboradores o terceros.

5.39. Zonas de entrega y carga: Espacio físico en las instalaciones del SENCICO donde se ejecuta la entrega de bienes y materiales por parte de contratistas, así como la carga de bienes y materiales para su envío a otras dependencias del SENCICO o a terceros.

6. ABREVIATURAS

6.1. OSCD: Oficial de Seguridad y Confianza Digital

6.2. SGSI: Sistema de Gestión de Seguridad de la Información

7. RESPONSABILIDADES

7.1. DE LA PRESIDENCIA EJECUTIVA

7.1.1. Implementar el SGSI

7.1.2. Aprobar los documentos normativos para implementar, operar, mantener y mejorar el SGSI.

7.2. DE LA GERENCIA GENERAL

7.2.1. Informar periódicamente al Presidente Ejecutivo del SENCICO los avances y dificultades en la implementación u operación del SGSI.

7.2.2. Informar el cumplimiento de la Resolución N° 003-2023-PCM/SGTD.

7.2.3. Asegurar el cumplimiento de las disposiciones establecidas en los documentos normativos del SGSI.

7.3. DEL COMITÉ DE GOBIERNO DIGITAL

7.3.1. Dirigir, mantener y supervisar estratégicamente los planes, resultados y recursos del SGSI.

7.3.2. Emitir opiniones o recomendaciones sobre la gestión estratégica del Sistema de Gestión de Seguridad de la Información (SGSI) a solicitud del titular de la entidad.

7.4. DE LOS GERENTES Y/O JEFES DE LAS UNIDADES DE ORGANIZACIÓN

7.4.1. Dentro de sus ámbitos de competencia, coadyuvar en la gestión de riesgos seguridad de la información e implementación de sus controles y en la gestión de incidentes de seguridad de la información identificados.

7.4.2. Establecer comunicación con autoridades para abordar temas relacionados con la seguridad de la información (DIVINDAT, entre otros). Esta comunicación se realiza mediante el uso de correo electrónico y otros medios disponibles para tal propósito. Estos contactos están registrados en el Anexo N° 07: Matriz de Contacto con Autoridades.

7.5. DE LA OFICINA DE PLANIFICACIÓN Y PRESUPUESTO

7.5.1. Orientar al Departamento de Informática para asegurar que la implementación y mantenimiento del SGSI del SENCICO esté articulado con los instrumentos de gestión institucional comprendidos en los sistemas administrativos de presupuesto público, planeamiento estratégico, programación multianual y gestión de inversiones con la implementación y mantenimiento del SGSI del SENCICO.

7.6. DEL DEPARTAMENTO DE RECURSOS HUMANOS

7.6.1. Fortalecer las competencias del personal de SENCICO en el uso adecuado, eficiente y seguro de las tecnologías digitales

7.6.2. Capacitar e informar al personal del SENCICO en temas de seguridad de la información y seguridad digital.

7.6.3. Asegurar que todos los colaboradores del SENCICO cumplan con la firma de los acuerdos de confidencialidad según el Anexo N° 08: Acuerdo de Confidencialidad, al momento de su ingreso.

7.7. DEL DEPARTAMENTO DE INFORMÁTICA

7.7.1. Coordinar la implementación y mantenimiento del SGSI en el SENCICO, atendiendo las normas en materia de seguridad digital, confianza digital y gobierno digital.

7.7.2. Informar a la SEGDI a través del Oficial de Seguridad y Confianza Digital (OSCD) todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda el SENCICO, de forma inmediata.

7.8. DE LOS USUARIOS

7.8.1. Aplicar en el ejercicio de sus funciones y actividades los conocimientos adquiridos en las capacitaciones en temas de Seguridad de la Información.

7.8.2. Cumplir con las disposiciones de esta directiva.

8. DISPOSICIONES GENERALES

8.1. DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El SGSI forma una parte esencial en las actividades del SENCICO, integrándose plenamente en su estructura. Asimismo, la seguridad de la información es

considerada durante el diseño de los procesos, sistemas y controles asociados, y el cumplimiento de sus requisitos es regido por las siguientes disposiciones:

8.1.1. El Comité de Gobierno Digital realiza el análisis de contexto a través de la identificación de los aspectos internos y externos relevantes para el SGSI de acuerdo con el Anexo N° 01: Análisis de Contexto del SENCICO.

8.1.2. El Comité de Gobierno Digital identifica las partes interesadas relevantes al SGSI, así como sus requisitos de seguridad de la información de acuerdo con el Anexo N° 02: Requisitos Relevantes para la Seguridad de la Información de las Partes Interesadas Relevantes para el SGSI.

8.1.3. El Comité de Gobierno Digital establece el alcance del SGSI, a nivel organizativo, técnico y físico y lo registra en el Anexo N° 03: Alcance del SGSI.

8.1.4. El Comité de Gobierno Digital define los objetivos del SGSI alineados a los objetivos estratégicos institucionales y considera los requisitos de seguridad de la información y la gestión de riesgos y oportunidades.

8.1.5. El Departamento de Recursos Humanos incluye las acciones de capacitación y concientización en seguridad de la información dentro del Plan de Desarrollo de las Personas y, asimismo, comparte con los nuevos colaboradores la normativa interna de seguridad de la información.

8.1.6. Las unidades de organización se encargan de compartir con los nuevos terceros a su cargo la normativa interna de seguridad de la información.

8.1.7. El Departamento de Informática coordina la ejecución de acciones de comunicación relevante al SGSI, tanto internas como externas.

8.1.8. La Oficina de Planificación y Presupuesto mantiene la información documentada del SGSI (política, directivas, procedimientos, entre otros) de acuerdo con la directiva establecida.

8.1.9. El Comité de Gobierno Digital establece el programa de operación del SGSI según el Anexo N° 04: Programa de Operación del Sistema de Gestión de Seguridad de la Información y coordina su ejecución.

8.1.10. Las unidades de organización realizan la medición de sus indicadores los cuales son presentados al Comité de Gobierno Digital para la evaluación del desempeño y efectividad del SGSI y toman acciones según sea el caso.

8.1.11. El Departamento de Informática coordina las auditorías internas al SGSI través de la ejecución del procedimiento establecido para tal fin.

8.1.12. El Comité de Gobierno Digital toma conocimiento de las no conformidades y oportunidades de mejora identificadas a través de auditorías al SGSI u

otras fuentes, y las comparte a las unidades de organización correspondientes para su atención.

8.1.13. Las unidades de organización establecen y coordinan las acciones sobre las no conformidades y oportunidades de mejora del SGSI identificadas usando el Anexo N° 05: Matriz de no Conformidades y Oportunidades de Mejora del SGSI.

8.1.14. El Comité de Gobierno Digital realiza la revisión del SGSI, previa preparación del informe por parte del Comité de Gobierno Digital según el Anexo N° 06: Informe para la Revisión del SGSI por la Alta Dirección, teniendo como resultado un acta de reunión de la revisión.

8.1.15. Por temas de seguridad de la información, es necesario que la carpeta de trabajo del equipo de cómputo cuente con respaldo de la aplicación One Drive (MS 365), para lo cual el usuario debe asegurarse que esté configurado.

8.2. DE LA SEGURIDAD DE LA INFORMACIÓN EN EL SENCICO

El SENCICO ha establecido las siguientes disposiciones para asegurar la adecuada protección de la información de la organización. Estas disposiciones tienen como objetivo definir los lineamientos para la designación de responsabilidades, la implementación de controles apropiados y la promoción de una cultura de seguridad en todos los niveles de la organización. Mediante la adopción de estas disposiciones, se busca garantizar la confidencialidad, integridad y disponibilidad de la información del SENCICO.

8.2.1. Las unidades de organización definen los grupos y roles necesarios para los accesos a la información tomando en consideración una adecuada definición y segregación de funciones de acuerdo con las actividades y funciones operativas que deban cumplir los distintos usuarios dentro de su unidad, la clasificación de los datos y la oposición de intereses entre las unidades de organización afectadas.

8.2.2. Las unidades de organización solicitan y autorizan los accesos a la información según los grupos y roles definidos..

8.2.3. El Departamento de Informática establece comunicación con el ente rector designado por la PCM para abordar temas relacionados con la seguridad de la información. Esta comunicación se realiza mediante el uso de correo electrónico y otros medios disponibles para tal propósito. Estos contactos están registrados en el Anexo N° 07: Matriz de Contacto con Autoridades.

8.2.4. Las unidades de organización se aseguran de que se incluyan cláusulas de confidencialidad en los términos de referencia para la contratación de servicios de terceros.

8.2.5. Las unidades de organización son responsables del cumplimiento de las disposiciones de la normativa interna en materia de seguridad de la información (políticas, directivas y procedimientos) por parte de los usuarios.

8.2.6. Las unidades de organización proporcionan las instrucciones necesarias para la adecuada utilización de los sistemas de información, aplicaciones y servicios.

8.3. DE LA ADMINISTRACIÓN DE ACTIVOS

La gestión de activos desempeña un papel fundamental en la protección de la información del SENCICO. Las responsabilidades relativas a la protección de los activos se encuentran bien definidas, respaldadas por pautas que regulan el uso adecuado de la información y las instalaciones de procesamiento.

8.3.1. Los Gerentes y/o jefes de las unidades de organización se aseguran de que todos los activos de información relevantes de su unidad, que estén en posesión de los usuarios a su cargo, sean devueltos al finalizar su relación contractual.

8.3.2. Las unidades de organización clasifican la información de su unidad en función del cumplimiento de los requisitos legales, su valor, criticidad y sensibilidad con el fin de prevenir su divulgación o modificación no autorizada.

8.4. DE LAS RELACIONES CON LOS CONTRATISTAS

Las relaciones con los contratistas implican riesgos para la seguridad de la información. Por tal motivo, se adoptan medidas de protección para establecer relaciones sólidas, transparentes y confiables con los contratistas, asegurando que compartan los valores de seguridad de la información y cumplan con los más altos estándares en la protección de los activos y datos del SENCICO.

8.4.1. Las unidades de organización aseguran la protección de los activos de información relevantes del SENCICO que puedan ser accedidos por los contratistas, a través de medidas de seguridad adecuadas que incluyen el establecimiento de acuerdos contractuales y cláusulas de confidencialidad.

8.4.2. Las unidades de organización se aseguran de que en los contratos con terceros se establezcan y acuerden todos los requisitos de seguridad

necesarios que se incluyen en el Anexo N° 14, para garantizar que los terceros solo puedan acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI de manera segura.

8.4.3. Las unidades de organización se aseguran de que los cambios en la provisión de servicios por parte de los terceros sean realizados preservando el cumplimiento de las políticas, directivas y procedimientos en materia de seguridad de la información. Se tiene en cuenta tanto la importancia de la información no pública como de los sistemas de información, aplicaciones y procesos implicados, realizando una reevaluación de los riesgos de seguridad de la información asociados a los servicios.

8.4.4. Los usuarios no están autorizados, bajo ninguna circunstancia, realizar cambios en el hardware, instalar software o modificar la configuración de los equipos informáticos.

9. DISPOSICIONES ESPECÍFICAS

9.1. DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

9.1.1. DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS PROYECTOS

Las unidades de organización consideran los temas relacionados con la seguridad de la información en los proyectos. Esto implica llevar a cabo una evaluación preliminar de los riesgos de seguridad de la información asociados al proyecto y el establecimiento de los roles y responsabilidades relacionados con la gestión de la seguridad de la información dentro del proyecto.

9.1.2. DE LOS DISPOSITIVOS MÓVILES

DE LA SEGURIDAD DE DISPOSITIVOS MÓVILES

a) El Departamento de Informática es el único autorizado para realizar cambios en el hardware, instalar software o modificar la configuración de los dispositivos móviles.
b) El Departamento de Informática gestiona la protección de los dispositivos móviles mediante una solución antimalware que se actualiza automáticamente.

DEL ALMACENAMIENTO DE INFORMACIÓN EN DISPOSITIVOS MÓVILES

a) Los usuarios no deben almacenar en los dispositivos móviles información no pública o que no sea estrictamente necesaria para el desarrollo de sus actividades.
b) El Departamento de Abastecimiento gestiona la desinstalación del software después de la devolución de un dispositivo móvil.

DE LA RESPONSABILIDAD DE LOS COLABORADORES

a) Los colaboradores son responsables de los dispositivos móviles asignados para el desempeño de sus actividades dentro y fuera de las instalaciones del SENCICO, por lo que deben garantizar la seguridad del equipo, así como de la información que contiene.
b) Los colaboradores notifican a la brevedad al Departamento de Informática si sospechan la infección por virus u otro software malicioso de un dispositivo móvil.
c) Los colaboradores deben informar de inmediato al Departamento de Abastecimiento en caso de robo o pérdida de los dispositivos móviles asignados, a fin de que se realicen las acciones necesarias.

9.1.3. DEL TRABAJO A DISTANCIA

DE LOS MEDIOS Y MECANISMOS PARA EL DESARROLLO DE TRABAJO A DISTANCIA

a) El Departamento de Informática brinda las facilidades necesarias para el acceso del colaborador a los sistemas de información, aplicaciones y servicios necesarios para el desarrollo de sus funciones cuando corresponda.
b) Los usuarios que desempeñen sus labores a distancia deben informar inmediatamente al Departamento de Abastecimiento sobre la pérdida, sustracción, deficiencia o deterioro de los medios y mecanismos otorgados por el SENCICO que hagan imposible su uso, a fin de adoptar medidas que garanticen la continuidad de sus labores.
c) Los usuarios deben ser los únicos que usen los medios y mecanismos asignados por el SENCICO para el trabajo a distancia, quedando estrictamente prohibido que otras personas hagan uso de éstos.

d) Los usuarios deben devolver al Departamento de Abastecimiento los medios y mecanismos asignados para el trabajo a distancia, en buen estado, al finalizar esta modalidad.
e) Los usuarios que desarrollen sus labores a distancia deben cumplir con la normativa interna de trabajo a distancia y la normativa en materia de seguridad de la información del SENCICO.

DE LA SEGURIDAD DE LA INFORMACIÓN EN EL TRABAJO A DISTANCIA

a) Los usuarios no deben permitir el acceso de terceros a información no pública del SENCICO.
b) Las unidades de organización gestionan la restricción de accesos a los sistemas de información y aplicaciones en caso de uso indebido o no autorizado.

9.2. DE LA ADMINISTRACIÓN DE ACTIVOS

9.2.1. DEL USO ACEPTABLE DE ACTIVOS

1. Las unidades de organización autorizan el acceso a los activos que son necesarios para la ejecución de las funciones de los usuarios.
2. Los usuarios no pueden conceder acceso ni compartir o transferir información no pública si no cuentan con la autorización respectiva.
3. Los usuarios no deben modificar o alterar información no pública sin la autorización de la unidad de organización a la que pertenecen.
4. Los usuarios no deben hacer uso de los activos de información para fines distintos a las funciones encomendadas.

9.2.2. DEL RETORNO DE ACTIVOS

1. Las unidades de organización se aseguran de que los usuarios, que utilizan sus propios equipos personales, realicen la transferencia segura de toda la información no pública de su unidad a los repositorios establecidos y posteriormente gestione la eliminación segura de la información contenida en estos equipos, al finalizar su relación contractual.
2. Las unidades de organización se aseguran de que, si los usuarios poseen conocimientos críticos para las operaciones de su unidad, estos sean documentados y transferidos para garantizar la continuidad al final de su relación contractual.

9.2.3. DEL ETIQUETADO DE LA INFORMACIÓN

1. Las unidades de organización se aseguran de que se etiqueten de manera clara y visible los documentos físicos y digitales de acuerdo con la clasificación de la información que contienen (siempre y cuando sean no públicos).

9.2.4. DEL MANEJO DE ACTIVOS

1. Las unidades de organización se aseguran de que los usuarios que tengan acceso a los activos de información clasificados como no públicos, tomen conocimiento de los mecanismos de protección definidos por su unidad.

9.2.5. DEL MANEJO DE MEDIOS REMOVIBLES

1. Las unidades de organización mantienen el registro de todos los medios removibles.
2. Las unidades de organización realizan el requerimiento de medios removibles al Departamento de Abastecimiento, precisando los usuarios, así como, el motivo del uso en cada caso.
3. El Departamento de Abastecimiento atiende los requerimientos de las unidades de organización y entrega los medios removibles.
4. Los usuarios deben devolver los medios removibles a las unidades de organización, cuando ya no los requieren.
5. Las unidades de organización registran la asignación y devolución de medios removibles y realizan el borrado seguro de estos según sea el caso.
6. Las unidades de organización envían el reporte de la asignación de medios removibles de manera semestral al Departamento de Informática usando el Anexo N° 09: Reporte de la Asignación de Medios Removibles.
7. Las unidades de organización se aseguran del borrado seguro de la información no pública que contienen los medios removibles.

9.2.6. DE LA TRANSFERENCIA DE MEDIOS FÍSICOS

1. El Departamento de Abastecimiento establece como requisito para la transferencia de medios físicos que contienen información no pública, que los transportes cumplan con la normativa interna vigente

en temas de trabajo a distancia, contrataciones, entre otros; para garantizar la seguridad de los activos frente a posibles daños físicos durante el tránsito.

2. El Departamento de Abastecimiento envía trimestralmente al Departamento de Informática el reporte de todas las transferencias de medios físicos que contienen información no pública a otras sedes (equipos de infraestructura de TI, entre otros). Este reporte es elaborado según el Anexo N° 10: Reporte de Transferencia de Medios Físicos a Otras Sedes.
3. El Departamento de Abastecimiento permite que s los equipos de infraestructura de TI sean retirados de su lugar solo con autorización previa de transferencia por parte del responsable de la unidad de organización responsable del equipo.
4. El Departamento de Abastecimiento ejecuta los retiros de los equipos de infraestructura de TI, siguiendo la directiva establecida para tal fin
5. Las unidades de organización son responsables de que la información no pública en formato físico no sea retirada del ambiente designado a otros ambientes dentro o fuera del SENCICO sin autorización previa del responsable de la unidad correspondiente.

9.3. DE LA SEGURIDAD FÍSICA Y AMBIENTAL

9.3.1. DE LAS ÁREAS SEGURAS

DEL PERÍMETRO DE SEGURIDAD FÍSICA

a) El Departamento de Abastecimiento tiene claramente definido el perímetro de seguridad física alrededor de las instalaciones del SENCICO para proteger sus activos.
b) El Departamento de Abastecimiento gestiona que se cuente con medidas de seguridad física para las instalaciones de procesamiento de información, para lo cual se cuenta con puertas de seguridad y sistemas de control de acceso, para regular y monitorear el ingreso y salida de personas y vehículos.

DE LOS CONTROLES DE INGRESO FÍSICO

a) La Secretaría General considera como medidas de seguridad para visitantes: el registro de entrada y salida, así como, el uso de tarjetas de identificación y notificación de su llegada a las unidades de organización.

b) Las unidades de organización brindan la concesión de accesos a sus visitantes de acuerdo con los propósitos específicos y realizan su escolta a las áreas seguras.

DEL ASEGURAMIENTO DE OFICINAS, ÁREAS E INSTALACIONES

a) Las unidades de organización restringen el acceso a las áreas donde se procesa o almacena información no pública, al personal autorizado por estas.
b) Las unidades de organización deben indicar a los usuarios sobre la existencia y restricciones dentro de las áreas seguras, según sea necesario.
c) Los usuarios autorizados deben ejecutar sus labores dentro del Data Center según lo establecido en el Instructivo de Seguridad y Correcto Uso de las Instalaciones de Procesamiento de la Información.

DE LA PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES

a) Las unidades de organización protegen las áreas seguras mediante controles de seguridad ambientales adecuados, basados en sistemas de control de temperatura y humedad, para proteger los activos de información relevantes.
b) Las unidades de organización realizan evaluaciones periódicas de la seguridad física y ambiental de las áreas seguras para identificar vulnerabilidades, implementar mejoras y garantizar el cumplimiento de las disposiciones.

DE LAS ZONAS DE ENTREGA Y CARGA

a) El Departamento de Abastecimiento controla y restringe el acceso a las zonas de entrega y carga, asegurando que solo el personal identificado y autorizado por las unidades de organización pueda ingresar.
b) Las unidades de organización controlan y restringen el acceso a las áreas seguras para que no puedan ser accesibles desde las zonas de entrega y carga, con el fin de prevenir el acceso no autorizado y proteger los activos de información relevantes.

9.3.2. DE LOS EQUIPOS Y OPERACIONES

DE LA SEGURIDAD DE EQUIPOS FUERA DE LAS INSTALACIONES

a) Las unidades de organización emplean medidas de protección física, para prevenir el robo, la pérdida o el daño de los equipos que contengan información no pública cuando se encuentren fuera de las instalaciones del SENCICO.
b) El Departamento de Abastecimiento mantiene un registro de los equipos de infraestructura de TI utilizados fuera de las instalaciones del SENCICO, incluyendo información sobre su ubicación, responsables y fechas de salida y retorno.

DE LOS EQUIPOS DE CÓMPUTO DESATENDIDOS

a) Los usuarios se aseguran de cerrar sesión en el sistema operativo, los sistemas de información, aplicaciones y servicios de red cuando ya no se necesiten.
b) Las unidades de organización protegen del uso no autorizado a los equipos de cómputo asignados a los usuarios, mediante un candado de seguridad con clave o un control equivalente.

DEL ESCRITORIO Y PANTALLA LIMPIOS

a) Las unidades de organización se aseguran de que los puestos de trabajo de los usuarios que procesan información no pública se encuentren localizados en ubicaciones que no queden expuestas al acceso de personas externas ajenas al SENCICO o personal no autorizado, para que de esta forma se protejan tanto los equipos de cómputo como la información no pública impresa que pudiera estar usando el personal.
b) Las unidades de organización se aseguran de que los equipos de cómputo que quedan ubicados cerca de zonas de atención o tránsito de público se sitúen de forma que las pantallas no puedan ser visualizadas por personas externas ajenas al SENCICO o personal no autorizado.
c) Los usuarios no deben mover ni trasladar equipos de cómputo (o componentes de equipos) del puesto de trabajo o de las instalaciones del SENCICO sin el visto bueno del Departamento de Informática.

d) Los usuarios no deben consumir alimentos o bebidas en las cercanías de los equipos de cómputo en caso almacene, procese o transmita información no pública.
e) Las unidades de organización proporcionan a sus usuarios muebles seguros (escritorio, caja fuerte, archivador u otro) con llave, para el resguardo de los documentos impresos, medios removibles y dispositivos móviles.
f) Los usuarios deben guardar bajo llave los documentos impresos, medios removibles y dispositivos móviles que contengan información no pública cuando no se estén utilizando, especialmente al finalizar la jornada laboral o cuando el personal se ausente de su puesto de trabajo.
g) Los usuarios no deben anotar sus credenciales (usuario y contraseña) de acceso a los sistemas de información, aplicaciones o servicios de red en papeles, documentos ni en ningún otro tipo de soporte (post-it, cuadernos, etc.).
h) El Departamento de Informática configura todos los equipos de cómputo para que estos sean accedidos solamente a través de credenciales (usuario y contraseña).
i) El Departamento de Informática configura los equipos de cómputo asignados a los usuarios para que se bloquee automáticamente con un protector de pantalla tras un período de inactividad. Para restablecer la operación normal, los usuarios deben ingresar sus credenciales (usuario y contraseña).
j) Los usuarios deben bloquear el equipo de cómputo asignado (combinación de teclas ⊞+L o Ctrl+Alt+Supr o Ctrl+Alt+Del, etc.) o bien apagarlo cuando se ausenten de su puesto de trabajo.
k) Los usuarios deben apagar el equipo de cómputo asignado al finalizar su jornada laboral o cuando vayan a tener una ausencia prolongada.
l) Los usuarios deben recoger inmediatamente la información no pública dispuesta por las impresoras o escáneres luego de enviarla a imprimir o escanear.
m) Los usuarios deben dejar las salas de reunión y capacitación sin el material utilizado que pueda contener información no pública luego de su uso.

n) Los usuarios deben eliminar la información no pública copiada en los equipos de cómputo utilizados para presentaciones (si éstos fueran de uso común) al finalizar las presentaciones.
o) Los usuarios deben borrar toda la información no pública que se haya expuesto sobre las pizarras o pantallas interactivas luego de su uso.

DE LA SEGURIDAD EN LOS PROCEDIMIENTOS OPERATIVOS

a) Las unidades de organización son responsables de la documentación de procedimientos o instructivos operativos que incluyan las pautas de seguridad de la información para la ejecución de sus actividades (de ser requerido).

SOBRE EL REGISTRO Y EVALUACIÓN DE CAMBIOS

a) Las unidades de organización registran solicitudes de cambios en los procesos, instalaciones de procesamiento de información y sistemas que puedan afectar la seguridad de la información, usando el Anexo N° 11: Formato de Solicitud de Cambio.
b) La Oficina de Planificación y Presupuesto, en coordinación con las unidades de organización solicitantes y el Departamento de Informática, evalúan los cambios según su impacto operacional, técnico y de seguridad, y priorizan su ejecución según corresponda, además deciden si se aceptan o no los cambios, lo cual se registra usando el Anexo N° 11: Formato de Solicitud de Cambio.
c) La Oficina de Planificación y Presupuesto, en coordinación con las unidades de organización y el Departamento de Informática, planifican los cambios, identificando: a) los requisitos organizacionales, operacionales, técnicos y de seguridad a implementar, b) las actividades a realizar como parte de los cambios, c) las pruebas a realizar antes de la implementación de los cambios y d) el presupuesto requerido, lo cual es registrado en el Anexo N° 11: Formato de Solicitud de Cambio, y debe ser aprobado por parte de la Gerencia General o el Departamento de informática según corresponda.
d) La Oficina de Planificación y Presupuesto, en coordinación con las unidades de organización y el Departamento de Informática, definen los pasos para: a) la aprobación formal de la

implementación de los cambios, que incluye la verificación del cumplimiento de los requisitos de seguridad, b) el retroceso, aborto y/o recuperación cuando los cambios son incorrectos o ante la ocurrencia de eventos inesperados durante la implementación de los cambios y c) la comunicación de los detalles de los cambios a todas las personas pertinentes.

9.4. DE LOS EVENTOS, INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

1. Los usuarios informan al Departamento de Informática sobre posibles debilidades de seguridad de la información en los hardware, software, servicios de red, personal y sede del SENCICO, para su evaluación respectiva. Para facilitar la identificación de debilidades, se puede tomar como referencia el Anexo N° 12: Catálogo de debilidades.
2. Los usuarios informan al Departamento de Informática sobre posibles incidentes de seguridad de la información, según el procedimiento establecido para tal fin. Para facilitar la identificación de incidentes, se puede tomar como referencia el Anexo N° 13: Catálogo de incidentes.
3. El Departamento de Informática verifica la naturaleza de los incidentes de seguridad reportados para determinar si son de tipo informático, en cuyo caso, procede a su atención; caso contrario lo deriva a las unidades de organización pertinentes para su atención según el procedimiento establecido para tal fin.
4. Las unidades de organización solicitan formalmente la investigación administrativa en aplicación del Reglamento Interno de Trabajo al Departamento de Recursos Humanos en caso de detectar acciones malintencionadas por parte de los colaboradores responsables de los incidentes de seguridad.

9.5. DE LA RELACIÓN CON LOS CONTRATISTAS

9.5.1. DE LA SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON LOS CONTRATISTAS

DE LA SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON LOS CONTRATISTAS

a) Las unidades de la organización definen los requisitos de seguridad de la información en los términos de referencia para mitigar los riesgos asociados al acceso o procesamiento de activos de

información del SENCICO para los bienes y servicios provistos por los proveedores. Para la definición de estos requisitos se deben tener en consideración los definidos en el Anexo N° 14: Lista Estándar de Requisitos de Seguridad de la Información para Contratos con Contratistas.

b) Las unidades de organización deben establecer en los acuerdos con contratistas que los requisitos de seguridad de la información deben ser aplicados también a su personal y subcontratistas, según sea el caso.

c) Los contratistas están autorizados exclusivamente para llevar a cabo las actividades contempladas en el contrato, en consecuencia, se establece que todas las acciones realizadas por su personal y subcontratistas están delimitadas a estas actividades.

d) Las unidades de organización deben solicitar las altas y bajas de los accesos a los sistemas de información, aplicaciones y servicios de red para los contratistas exclusivamente solo al entorno relacionado con la prestación del servicio y, asimismo, deberían ser caducados en forma inmediata a la finalización del servicio contratado.

9.5.2. DE LA GESTIÓN DE ENTREGA DE SERVICIOS DEL CONTRATISTA

DEL MONITOREO Y REVISIÓN DE SERVICIOS QUE BRINDAN LOS CONTRATISTAS

a) Las unidades de organización se encargan del monitoreo regular del cumplimiento del contrato de los servicios críticos de contratistas en cuanto a las cláusulas contractuales de seguridad de información, incluyendo las relacionadas a acuerdos de niveles de servicio.

b) Las unidades de organización llevan a cabo la revisión regular de los informes de los servicios críticos generados por los contratistas, los cuales deben incluir el cumplimiento de las cláusulas contractuales de seguridad de información, incluyendo las relacionadas a acuerdos de niveles de servicio.

c) Las unidades de organización coordinan la realización de auditorías a los servicios críticos que brindan los contratistas, directamente o a través de auditores independientes, teniendo como criterio de auditoría el nivel de cumplimiento de las cláusulas contractuales de seguridad de la información.

d) Las unidades de organización se aseguran de que los riesgos o problemas identificados durante los monitoreos, revisiones o auditorías a los servicios críticos de contratistas, sean resueltos y gestionados de manera oportuna asegurando la implementación de acciones correctivas o de mejora adecuadas.

DE LA GESTIÓN DE CAMBIOS A LOS SERVICIOS DE CONTRATISTAS

a) Las unidades de organización gestionan los cambios que pudieran surgir en la prestación de los servicios críticos para las operaciones del SENCICO según los acuerdos contractuales establecidos con los contratistas, asegurando que las modificaciones estén alineadas con la normativa interna de seguridad de la información y la normativa de contrataciones del estado.
b) Las unidades de organización deben evaluar si los cambios que pudieran surgir en la prestación de los servicios críticos para las operaciones del SENCICO, involucran nuevos riesgos de seguridad de la información por el acceso o procesamiento de información por parte de los contratistas, en cuyo caso se podrían incluir o modificar cláusulas contractuales de seguridad de la información para mitigarlos y preservar la continuidad de los servicios.

9.6. DEL CUMPLIMIENTO

9.6.1. DEL CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

1. La Gerencia General mantiene un registro de los requisitos legales, estatutarios, regulatorios y contractuales relacionadas a la seguridad de la información, según el Anexo N°15: Matriz de Requisitos Normativos y Contractuales Relacionados a Seguridad de la Información.
2. Las unidades de organización deben cumplir con los requisitos de propiedad intelectual adoptando las siguientes disposiciones:
    a) Hacer uso legal del software e información (impresa y digital).
    b) Adquirir software e información (impresa y digital) mediante fuentes fiables y de buena reputación.
    c) Identificar todo el software e información (impresa y digital) con los requisitos para proteger los derechos de propiedad intelectual.

3. El Departamento de Informática debe cumplir con los requisitos de propiedad intelectual adoptando las siguientes disposiciones:
    a) Mantener pruebas y evidencias de la propiedad de las licencias de software adquiridas.
    b) Configurar políticas para garantizar que no se exceda el número permitido de usuarios de las licencias de software.
4. Los usuarios no deben realizar la duplicación, transformación ni copia total o parcial de la información (impresa y digital), sin que lo permita la ley de derechos de autor.
5. Las unidades de organización deben identificar los registros (información impresa y digital) y sus tiempos de retención, según los requisitos legales establecidos.
6. El Departamento de Informática debe proveer soporte para que la retención, almacenamiento, preservación, manipulación y eliminación de registros (información digital) se realice manera segura según lo requerido por las unidades de organización.
7. El Departamento de Informática apoya en la implementación de las medidas de seguridad técnicas establecidas en la normativa en materia de protección de datos personales.
8. El Departamento de Informática debe considerar restricciones regulatorias sobre el uso de controles criptográficos antes de implementarlos.

9.6.2. DE LAS REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

DE LA REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

a) La Oficina de Planificación y Presupuesto coordina la ejecución de revisiones periódicas independientes al SGSI según la ISO/IEC 27001 mediante auditorías externas anuales que son realizadas por un proveedor de servicios de auditoría. Los hallazgos de la revisión independiente son comunicados al Comité de Gobierno Digital para que evalúe las acciones correctivas o mejoras necesarias que deben ser implementadas por las unidades de organización.

b) La Oficina de Planificación y Presupuesto debe observar que las auditorías externas al SGSI según la ISO/IEC 27001 sean realizadas por el proveedor siguiendo los formatos establecidos

del procedimiento de auditorías internas del SENCICO, siempre y cuando no se trate de auditorías de certificación ISO/IEC 27001.

DEL CUMPLIMIENTO DE LA NORMATIVA INTERNA DE SEGURIDAD DE LA INFORMACIÓN

a) Las unidades de organización deben cumplir con la normativa interna de seguridad de la información (política, directivas y procedimientos) e informar oportunamente en caso de incumplimiento.
b) Las unidades de organización deben consultar cualquier inquietud o duda que generase la aplicación o interpretación de la normativa interna de seguridad de la información al Departamento de Informática.

9.7. DE LA CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

1. La Oficina de Planificación y Presupuesto incluye los requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información, en situaciones adversas, dentro del Plan de Continuidad Operativa del SENCICO.
2. La Oficina de Planificación y Presupuesto debe establecer, documentar, implementar y mantener procedimientos y controles dentro del Plan de Continuidad Operativa del SENCICO para asegurar que se obtenga el nivel requerido de seguridad de la información durante una situación adversa.
3. La Oficina de Planificación y Presupuesto debe verificar, dentro de las pruebas y mantenimiento del Plan de Continuidad Operativa del SENCICO, los procedimientos y controles de continuidad de seguridad de la información establecidos como parte de él.

X. ANEXOS

1. **Anexo N° 01** “Análisis de Contexto del SENCICO
2. **Anexo N° 02** “Requisitos Relevantes para la Seguridad de la Información de las Partes Interesadas Relevantes para el SGSI
3. **Anexo N° 03** “Alcance del SGSI”
4. **Anexo N° 04** “Programa de Operación del Sistema de Gestión de Seguridad de la Información”

5. **Anexo N° 05** “Matriz de No Conformidades y Oportunidades de Mejora del SGSI”
6. **Anexo N° 06** “Informe de revisión del SGSI por la Alta Dirección”
7. **Anexo N° 07** “Matriz de contacto con Autoridades”
8. **Anexo N° 08** “Acuerdo de Confidencialidad”
9. **Anexo N° 09** “Reporte de Asignación de Medios Removibles”
10. **Anexo N° 10** “Reporte de Transferencia de Medios Físicos a Otras Sedes”
11. **Anexo N° 11** “Formato de Solicitud de Cambio”
12. **Anexo N° 12** “Catálogo de debilidades”
13. **Anexo N° 13** “Catálogo de incidentes”
14. **Anexo N° 14** “Lista Estándar de Requisitos de Seguridad de la Información para Contratos con Contratistas”
15. **Anexo N° 15** “Matriz de Requisitos Normativos y Contractuales Relacionados a Seguridad de la Información”

Anexo N° 01
Análisis de Contexto del SENCICO

1. INTRODUCCIÓN

El objetivo del análisis de contexto es obtener una visión general del SENCICO, considerando factores del entorno interno y externo que puedan afectar la seguridad de la información.

2. SENCICO

2.1. Misión

[Especificar la misión del SENCICO indicada en el Plan Estratégico Institucional].

2.2. Visión

[Especificar la visión del SENCICO indicada en el Plan Estratégico Institucional].

2.3. Objetivos estratégicos

[Especificar los objetivos estratégicos del SENCICO indicados en el Plan Estratégico Institucional].

2.4. Acciones estratégicas

[Especificar las acciones estratégicas del SENCICO indicadas en el Plan Estratégico Institucional].

3. ENTORNO EXTERNO

En el análisis del entorno externo se identifican y analizan a nivel general los aspectos externos que afectan la seguridad de la información.

A continuación, se describe la información del entorno externo del SENCICO, consolidada en las siguientes categorías:

- Social y cultural.
- Político.
- Legal, normativo y regulatorio.
- Financiero y macroeconómico.
- Tecnológico.
- Natural.
- Competitivo.

3.1. Información revisada sobre aspectos externos según categorías

3.1.1. [Categoría de aspectos externos]

[Información revisada según la categoría de aspectos externos …]

3.2. Aspectos externos

[Realizar un análisis de la información recabada sobre el entorno externo e identificar los aspectos externos]

Categoría	Aspecto externo
[Categoría del aspecto].	[Especificar el aspecto externo].
[…]	[…]

4. ENTORNO INTERNO

A continuación, se describe la información del entorno interno del SENCICO, consolidada en las siguientes categorías:

[

- Cultura organizacional.
- Políticas, objetivos y estrategias.
- Gobernanza, estructura organizacional, roles y responsabilidades.
- Normas, directrices y modelos adoptados por el SENCICO.
- Relaciones contractuales que pueden afectar directamente los procesos incluidos en el alcance del SGSI.
- Procesos y procedimientos.
- Capacidades, en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías).
- Infraestructura física y entorno.
- Sistemas de información, flujos de información y procesos de toma de decisiones (tanto formal como informal).
- Auditorías previas y resultados previos de evaluación de riesgos.

]

4.1. Información revisada sobre aspectos internos según categorías

4.1.1. [Categoría de aspectos internos]

[Información revisada según la categoría de aspectos internos …]

4.2. Aspectos internos

[Realizar un análisis de la información recabada sobre el entorno interno e identificar los aspectos internos]

Categoría	Aspecto interno
[Categoría del aspecto].	[Especificar el aspecto interno].
[…]	[…]

Anexo N° 02
Requisitos Relevantes para la Seguridad de la Información de las Partes Interesadas Relevantes para el SGSI

1. INTRODUCCIÓN

El objetivo del documento de requisitos relevantes para la seguridad de la información de las partes interesadas relevantes para el SGSI, es identificar las personas, grupos u organizaciones relevantes para el Sistema de Gestión de la Seguridad de la Información (SGSI) y sus respectivos requisitos relevantes para la seguridad de la información, los cuales deben ser plenamente comprendidos para garantizar que los procesos y controles de seguridad sean los adecuados para sus necesidades y expectativas.

2. PARTES INTERESADAS EXTERNAS

A continuación, se describe la información recabada sobre las necesidades y expectativas de las siguientes partes interesadas externas:

[
- Reguladores y legisladores.
- Accionistas, incluidos propietarios e inversores.
- Proveedores que incluyen subcontratistas, consultores y socios externos.
- Asociaciones industriales.
- Competidores.
- Clientes y consumidores.
- Grupos activistas.

]

2.1. Información revisada sobre necesidades y expectativas de partes interesadas externas

2.1.1. [Parte interesada externa]

[Información de la parte interesada externa …]

2.2. Requisitos de partes interesadas externas

[Realizar un análisis de la información recabada sobre las partes interesadas externas e identificar los requisitos de estas partes interesadas]

Parte Interesada	Requisitos	
	Necesidades	Expectativas
[Parte interesada].	[Especificar las necesidades de la parte interesada]	[Especificar las expectativas de la parte interesada]

Parte Interesada	Requisitos	
	Necesidades	Expectativas
[…]	[…]	

3. PARTES INTERESADAS INTERNAS

A continuación, se describe la información recabada sobre las necesidades y expectativas de las siguientes partes interesadas internas:

[

- Tomadores de decisiones, incluyendo la alta dirección.
- Propietarios de proceso, propietarios de sistema y propietarios de la información.
- Funciones de soporte tales como TI o Recursos Humanos.
- Empleados y usuarios.
- Profesionales de seguridad de la información.

]

3.1. Información revisada sobre necesidades y expectativas de partes interesadas internas

3.1.1. [Parte interesada interna]

[Información de la parte interesada interna …]

3.2. Requisitos de partes interesadas internas

[Realizar un análisis de la información recabada sobre las partes interesadas internas e identificar los requisitos de estas partes interesadas]

Parte Interesada	Requisitos	
	Necesidades	Expectativas
[Parte interesada].	[Especificar las necesidades de la parte interesada]	[Especificar las expectativas de la parte interesada]
[…]	[…]	

Anexo N° 03
Alcance del SGSI

1. OBJETIVO

El objetivo del documento es definir claramente los límites y aplicabilidad del Sistema de Gestión de Seguridad de la Información (SGSI) en el SENCICO.

2. ALCANCE DEL SGSI

A fin de establecer el alcance del SGSI, se enfocó en los [macroprocesos / procesos] con mayor aporte a los objetivos estratégicos del SENCICO para proteger sus respectivos activos de información. El SENCICO determina el siguiente alcance para el SGSI:

[Texto del alcance del SGSI]

A nivel organizativo, técnico y físico el alcance se detalla de la siguiente manera:

2.1. Alcance Organizativo

2.1.1. [Macroprocesos / procesos]

[Alcance y límites].

2.1.2. [Áreas y/o personal]

[Alcance y límites].

2.2. Alcance Técnico

2.2.1. [Hardware]

[Alcance y límites].

2.2.2. [Software]

[Alcance y límites].

2.2.3. [Redes]

[Alcance y límites].

2.2.4. [Comunicaciones]

[Alcance y límites].

2.2.5. [Servicios de TIC]

[Alcance y límites].

2.3. Alcance Físico

2.3.1. [Oficinas]

[Alcance y límites].

2.3.2. [Ubicaciones]

[Alcance y límites].

2.3.3. [Instalaciones]

[Alcance y límites].

2.4. Interfaces y dependencias entre actividades del SENCICO y otras organizaciones

Macroproceso / proceso	Dependencia	Interfaces
[Alcance y límites].	[Especificar las dependencias].	[Especificar las interfaces con las dependencias]
[…]	[…]	

Anexo N° 04
Programa de Operación del Sistema de Gestión de Seguridad de la Información

Nº	Fase	Actividad	AÑO 20XX											
			I Trimestre			II Trimestre			III Trimestre			IV Trimestre		
			ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SET	OCT	NOV	DIC

Anexo N° 05
Matriz de No Conformidades y Oportunidades de Mejora del SGSI

Identificación de NC u OM															Evaluación de NC u OM					Implementación (por Unidad Orgánica, sobre correcciones, acciones correctivas o acciones de mejora)			Seguimiento (por OSD, sobre correcciones, acciones correctivas o acciones de mejora)			Evaluación de la eficacia (por OSD, sobre correcciones, acciones correctivas o acciones de mejora)				
N°	Proceso	Unidad Orgánica involucrada	Código	Tipo de hallazgo		Fecha de presentación del hallazgo o acuerdo	Origen						Descripción de la NC u OM	Consecuencias de la NC u OM	Descripción de la corrección o acción de mejora	Causa raíz del hallazgo (obligatorio en caso de NC)	Descripción de la acción correctiva (obligatorio en caso de NC)	Responsable de la implementación	Fecha programada de implementación	Acciones implementadas	Responsable de la acción implementada	Fecha de implementación de la acción	Descripción del seguimiento	Fecha del seguimiento	Responsable del seguimiento	¿La acción correctiva fue eficaz?	Descripción de la eficacia	Responsable de evaluación de la eficacia	Fecha de evaluación de la eficacia	Estado
				No conformidad	Oportunidad de mejora		Auditoría interna	Auditoría externa	Revisión por la Dirección	Riesgos y oportunidades de SI	Monitoreo, medición, análisis y evaluación	Hallazgos de personal																		
1																													
2																													
3																													
4																													

Anexo N° 06
Informe para la Revisión del SGSI por la Alta Dirección

1. INTRODUCCIÓN

Presentar los resultados de la operación del Sistema de Gestión de Seguridad de Información (SGSI) del SENCICO, correspondiente al período del [dd/mm/aaaa] al [dd/mm/aaaa], para la revisión de su idoneidad, adecuación y eficacia continua.

2. ESTADO DE LOS ACUERDOS DE LAS REVISIONES ANTERIORES

<Resumen sobre el estado de implementación de los acuerdos de las revisiones anteriores>

N°	Acuerdo	Plazo	Estado (Implementado/ En Proceso/ Pendiente)
[N°]	[Descripción del acuerdo]	[Plazo de implementación del acuerdo]	[Estado del acuerdo]
[…]			

3. CAMBIOS RELEVANTES EN LOS ASPECTOS INTERNOS Y EXTERNOS

<Resumen sobre los cambios en los aspectos internos y externos (nuevos, modificados o eliminados)>

Factores Externos	Factores Internos
[Cambios en los aspectos externos]	[Cambios en los aspectos internos]
[…]	

4. RETROALIMENTACIÓN SOBRE EL DESEMPEÑO DE LA SEGURIDAD DE LA INFORMACIÓN

4.1. No Conformidades y Acciones Correctivas

<Resumen sobre el estado de implementación de las acciones correctivas y las principales acciones correctivas>

Origen	N° Total	N° Pendiente	N° En Proceso	N° Implementada
[Fuente de detección: auditoría interna / auditoría externa / revisión	[N° total de acciones correctivas por origen]	[N° de acciones correctivas pendientes de implementar del N° total de acciones	[N° de acciones correctivas en proceso de implementación del N° total de acciones	[N° de acciones correctivas implementadas del N° total de acciones

Origen	N° Total	N° Pendiente	N° En Proceso	N° Implementada
por la dirección / riesgos y oportunidades de seguridad de la información / monitoreo, medición, análisis y evaluación / hallazgos de personal].		correctivas por origen]	correctivas por origen]	correctivas por origen]
[…]	[…]			

4.2. Resultados del monitoreo y medición

<Resumen sobre los resultados del monitoreo y medición>

Código	Nombre	Meta	Resultado Trimestre 1	Resultado Trimestre 2	Resultado Trimestre 3	Resultado Trimestre 4
[Código del indicador].	[Nombre del indicador]	[Meta del indicador]	[Resultado para el trimestre 1 del indicador]	[Resultado para el trimestre 2 del indicador]	[Resultado para el trimestre 3 del indicador]	[Resultado para el trimestre 4 del indicador]
[…]			[…]			

4.3. Resultados de auditoría

<Resumen sobre los resultados de auditoría y los principales hallazgos encontrados>

Auditoría	Fecha de Inicio	N° No Conformidades	N° Observaciones	N° Oportunidades de Mejora
[Descripción de la auditoría].	[Fecha de inicio de la auditoría]	[N° de no conformidades identificadas en la auditoría]	[N° de observaciones identificadas en la auditoría]	[N° de oportunidades de mejora

Auditoría	Fecha de Inicio	N° No Conformidades	N° Observaciones	N° Oportunidades de Mejora
				identificadas en la auditoría]
[…]				

4.4. Cumplimiento de los objetivos del SGSI

<Resumen sobre el cumplimiento de los objetivos del SGSI en función a los resultados del monitoreo y medición>

5. RETROALIMENTACIÓN DE LAS PARTES INTERESADAS

<Resumen sobre la retroalimentación de las partes interesadas, incluidas sugerencias para mejoras, solicitudes de cambio y quejas>

Parte Interesada	Retroalimentación
[Descripción de la parte interesada].	[Retroalimentación]
[…]	

6. RESULTADOS DE LA GESTIÓN DE RIESGOS

<Resumen sobre los resultados de la gestión de riesgos, el estado del plan de tratamiento de riesgos y del plan de acción de oportunidades>

Gestión de Riesgos			
Proceso / Función / Servicio	**N° Riesgos Evaluados**	**N° Riesgos Tolerables**	**N° Riesgos no Tolerables**
[Nombre de proceso / función / servicio]	[N° de riesgos evaluados para el proceso / función / servicio]	[N° de riesgos tolerables dentro de los riesgos evaluados]	[N° de riesgos no tolerables dentro de los riesgos evaluados]
[…]			

Plan de Tratamiento - Riesgos				
Proceso / Función / Servicio	**N° Total**	**N° de Pendientes**	**N° En Proceso**	**N° Implementados**
[Nombre de proceso /	[N° total de controles en	[N° de controles	[N° de controles en	[N° de controles

Plan de Tratamiento - Riesgos				
Proceso / Función / Servicio	**N° Total**	**N° de Pendientes**	**N° En Proceso**	**N° Implementados**
función / servicio]	el plan de tratamiento para el proceso / función / servicio]	pendientes de implementar en el plan de tratamiento]	proceso de implementación en el plan de tratamiento]	implementados en el plan de tratamiento]
[…]				

Plan de Acción – Oportunidades				
Proceso / Función / Servicio	**N° Total**	**N° de Pendientes**	**N° En Proceso**	**N° Implementados**
[Nombre de proceso / función / servicio]	[N° total de oportunidades en el plan de tratamiento para el proceso / función / servicio]	[N° de oportunidades pendientes de implementar en el plan de tratamiento]	[N° de oportunidades en proceso de implementación en el plan de tratamiento]	[N° de oportunidades implementadas en el plan de tratamiento]
[…]				

7. OPORTUNIDADES DE MEJORA

<Resumen sobre el estado de implementación de las oportunidades de mejora y las principales oportunidades de mejora>

Origen	N° Total	N° Pendiente	N° En Proceso	N° Implementada
[Fuente de detección: auditoría interna / auditoría externa / revisión por la dirección / riesgos y oportunidades de seguridad	[N° total de oportunidades de mejora por origen]	[N° de oportunidades de mejora pendientes de implementar del N° total de oportunidades de mejora por origen]	[N° de oportunidades de mejora en proceso de implementación del N° total de oportunidades de mejora por origen]	[N° de oportunidades de mejora implementadas del N° total de oportunidades de mejora por origen]

Origen	N° Total	N° Pendiente	N° En Proceso	N° Implementada
de la información / monitoreo, medición, análisis y evaluación / hallazgos de personal].				
[…]	[…]			

Anexo N° 07
Matriz de Contacto con Autoridades

N°	Nombre de la entidad	Descripción de la entidad	Contactos de la entidad	Medios de contacto con la entidad	Materias involucradas
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Anexo N° 08
Acuerdo de Confidencialidad

Conste por el presente documento que yo: …… ……, identificado(a) con D.N.I. Nº ……, domiciliado(a) en …….. que como consecuencia de la labor que desempeño en el Servicio Nacional de Capacitación para la Industria de la Construcción (SENCICO) y teniendo acceso a información, cuyo término significa cualquier información escrita, gráfica, oral, electromagnética o de cualquier otro tipo, de propiedad del SENCICO, me comprometo indefinidamente a:

1. Mantener la información en estricta reserva y confidencialidad, no divulgarla acto alguno de la información a otra persona, ya sea natural o jurídica.
2. No usar la información directa o indirectamente en beneficio propio o de terceros, excepto para cumplir a cabalidad mis funciones relacionadas al puesto que desempeño.
3. No revelar total o parcialmente a otra persona, ya sea natural o jurídica, la información obtenida como consecuencia directa o indirecta de las conversaciones y/o de la prestación de servicios en el puesto que desempeño.
4. No utilizar unidades removibles y/o computadoras portátiles, sin autorización escrita del SENCICO y en caso contrario, sólo para los fines que me fueron autorizados.
5. No enviar a otra persona, ya sea natural o jurídica, archivos que contengan información de propiedad del SENCICO a través de correo electrónico, servicios en la nube u otros medios a los que tenga acceso, sin la autorización respectiva.

Asimismo, dejo constancia que tengo conocimiento de lo establecido por la normatividad referida a “Seguridad de la información”, la cual me comprometo a cumplir.

Así, en caso de incumplimiento de lo estipulado en el presente documento, me someto a las sanciones contenidas en las normas generales e instrumentos internos vigentes del SENCICO aplicables a mi modalidad contractual.

Para constancia de lo anterior, suscrito entre este acuerdo de confidencialidad en pleno uso de mis facultades, a los …… días de…… del año…….

…….
FIRMA

DNI N° ……

Huella dactilar

Anexo N° 09
Reporte de la Asignación de Medios Removibles

N°	Código	Tipo de medio (*)	Nombre de medio	Descripción de medio	Asignado a	Estado (**)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

(*) Tipo de medio: Disco duro externo, Cinta magnética, Medio óptico CD, Medio óptico CD-RW, Medio óptico DVD, Medio óptico Blu-ray, Otro medio óptico, Memoria USB, Memoria SD, Memoria SDHC, Otra memoria
(*) Estado: Disponible, Asignado, Eliminado

Anexo N°10
Reporte de Transferencia de Medios Físicos a Otras Sedes

N°	Código	Tipo de medio (*)	Nombre de medio	Descripción de medio	Enviado desde:	Enviado hacia:	Fecha

(*) Tipo de medio: Equipos de cómputo, Servidores, Equipos de redes y comunicaciones, Equipos de seguridad

Anexo N° 11
Formato de Solicitud de Cambio

(A SER LLENADO POR EL SOLICITANTE)

1. IDENTIFICACIÓN Y REGISTRO	
Código de solicitud	S-[aaaa]-[mm]-[dd]
Nombre del solicitante	
Unidad solicitante	
Fecha de solicitud	
Tipo de cambio	☐ Procesos de negocio. ☐ Instalaciones de procesamiento de información. ☐ Sistemas (software).
Descripción del cambio propuesto	
Razón del cambio	
Anexos / referencias	
Firma del solicitante	

2. EVALUACIÓN	
Impacto operacional	[procesos, procedimientos, etc.]
Impacto técnico	[instalaciones de procesamiento de información, infraestructura, sistemas]
Impacto en seguridad	[confidencialidad, integridad y disponibilidad de la información]

3. PRIORIZACIÓN	
Prioridad	☐ Baja: Se necesita el cambio, pero puede esperar hasta un mejor momento. ☐ Normal: No representa una urgencia o no implica un impacto importante, pero no se debe diferir el cambio. ☐ Alta: Se necesita implementar el cambio de manera oportuna, sino se puede afectar el cumplimiento o las operaciones críticas. ☐ Máxima: Se necesita con urgencia el cambio, ya que se afecta el cumplimiento o las operaciones críticas.

4. ACEPTACIÓN	
¿Se acepta el cambio?	☐ Sí ☐ No
Justificación de decisión	
Fecha de decisión	
Nombre del decisor	
Firma del decisor	

5. PLANIFICACIÓN				
Requisitos				
N°	**Descripción**		**Tipo**	
			[operacional, técnico, seguridad]	
Actividades				
N°	**Descripción**	**Responsable**	**Fecha de inicio**	**Fecha de fin**
Pruebas				
N°	**Descripción**	**Responsable**	**Fecha de inicio**	**Fecha de fin**
Presupuesto				
N°	**Ítem**	**Responsable**	**Fecha**	**Costo**
Total				
Nombre del aprobador del plan				
Firma del aprobador				

6. PASOS	
Aprobación formal	[descripción de los pasos de aprobación formal para la implementación de los cambios, el cual, debe incluir la verificación de que se han cumplido los requisitos]
Retroceso	[descripción de los pasos de retroceso, incluido el procedimiento para abortar y recuperar los cambios incorrectos y los eventos inesperados]
Comunicación	[descripción de los pasos de comunicación de los detalles de los cambios a todas las personas pertinentes]

Anexo N° 12

Catálogo de debilidades

Categoría	Casos
Hardware	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento.
	Falta de esquemas de reemplazo periódicos.
	Almacenamiento no protegido.
	Disposición o reutilización de medios removibles sin borrar apropiadamente
	Falta de cuidado al descartarlo.
Software	Equipos de cómputo sin antivirus instalado.
	Copia no controlada.
	Pruebas al software inexistentes o insuficientes.
	Errores en el software.
	Falta de evidencias de auditoría.
	Asignación equivocada de derechos de acceso.
	Falta de documentación
	Configuración incorrecta de parámetros
	Falta de mecanismos de identificación y autentificación de usuarios.
	Mala administración y protección de contraseñas.
	Habilitación de servicios innecesarios.
	Falta de control de cambios eficaz.
	Descarga y uso incontrolado de software.
	Falta de copias de respaldo.
Servicios de red	Juntas malas en el cableado de red.
	Falta de identificación y autentificación de emisor y destinatario.
	Transferencia de contraseñas sin cifrado.
	Tráfico delicado no protegido contra intercepción.
	Conexiones no protegidas a la red pública.
Personal	Capacitación de seguridad insuficiente.
	Uso incorrecto del software y hardware.
	Falta de conciencia de seguridad.
	Falta de mecanismos de monitoreo.
	Trabajo no supervisado del personal externo o de limpieza.
Sede	Falta de protección física del edificio, puertas y ventanas
	Uso inadecuado o negligente del control de acceso físico a edificios y oficinas.
	Ubicaciones en un área susceptible a las inundaciones.
	Red inestable de energía eléctrica.

Anexo N° 13

Catálogo de incidentes

Descripción	Casos	Tipo
Mal uso de correo	Envío de cadenas, spam, vídeo, música, entre otros.	Seguridad digital
Mal uso de internet	Acceso a páginas prohibidas, cargas y descargas no autorizadas, consultas de interés no organizacional, entre otros.	Seguridad digital
Mal uso de estaciones de trabajo	Uso para juegos o música, entre otros.	Seguridad digital
Mal uso de cuentas de usuario	Préstamo de cuentas, uso de cuentas ajenas, entre otros.	Seguridad de la información
Carpetas mal compartidas	Carpetas abiertas sin restricción, entre otros	Seguridad de la información
Software no autorizado	Instalación o uso no autorizado de software, entre otros	Seguridad digital
Hardware no autorizado	Conexión o uso no autorizado de equipos y dispositivos en la red, entre otros	Seguridad digital
Accesos lógicos no autorizados	Accesos indebidos o no autorizados a sistemas de información o bases de datos a través del uso de artificios, intrusión, entre otros.	Seguridad digital
Robo de información digital	Retiro no autorizado de información en USB u otros medios removibles.	Seguridad de la información
Alteración de la información	Eliminación o modificación no autorizada de archivos, registros, entre otros.	Seguridad digital
Divulgación no autorizada de la información	Publicaciones no autorizadas de la información, entre otros	Seguridad de la información
Ingeniería social	No cumplimiento de las disposiciones de escritorios y pantallas limpias, escritura de claves escritas en papel desatendidas, impresiones no recogidas, falta de ética en las comunicaciones, entre otros.	Seguridad de la información
Pérdida o robo de estaciones de trabajo y/o partes	Desaparición de estaciones de trabajo y partes, entre otros.	Seguridad de la información
Código malicioso	Existencia de virus, malware, entre otros.	Seguridad digital
Desastres naturales/vandalismo	Destrucción o afectación total o parcial de áreas de procesamiento de información, entre otros.	Seguridad de la información
Accesos físicos no autorizados	Acceso físico no autorizado al Data Center u otros recursos y/o instalaciones restringidas del SENCICO, entre otros.	Seguridad de la información
Pérdida o robo de información en formato físico	Retiro no autorizado de la información en formato físico fuera del perímetro del SENCICO, entre otros	Seguridad de la información
Falla de los sistemas de información	Falla o lentitud extrema de los sistemas de información, entre otros.	Seguridad digital

Descripción	Casos	Tipo
Cambios no autorizados en los sistemas de información	Cambios o modificaciones en los sistemas de información, entre otros.	Seguridad digital
Alteración de la página web institucional	Modificación o eliminación no autorizada de un sitio o página web del SENCICO, entre otros.	Seguridad digital
Falla en las comunicaciones	Falla o lentitud extrema en la red interna, correo electrónico, entre otros.	Seguridad digital

Anexo N° 14
Lista Estándar de Requisitos de Seguridad de la Información para Contratos con Contratistas

- Detalle de la información no pública que será accedida, cómo podrá ser accedida, así como, la clasificación y protección de esta.
- Obligación de que, una vez finalizado el contrato, el contratista ya no podrá acceder o mantener la información no pública del SENCICO.
- Cumplimiento de la legislación en materia de protección de datos personales y propiedad intelectual.
- Derecho de auditoría y de control sobre aspectos relevantes del contrato por parte del SENCICO sobre el contratista.
- Inclusión de situaciones que conlleven a la finalización del contrato.
- Penalizaciones por incumplimiento.
- Devolución de los activos de información a la finalización de la relación contractual.
- Detalle de controles técnicos:
    1. Implementación de mecanismos sólidos de acceso a la información.
    2. Cifrado de datos no públicos.
    3. Actualizaciones periódicas de controles de seguridad implementados para proteger la información.
    4. Control de acceso físico a los ambientes donde se encuentra la información.
    5. Observancia de disposiciones de uso aceptable de la información.
    6. Procesos de gestión de problemas e incidentes de seguridad.
    7. Acuerdos de nivel de servicio (errores y faltas permitidas, indisponibilidad del servicio, tiempo de atención de incidentes, entre otros).
    8. Uso de equipos de cómputo del SENCICO con las condiciones respectivas para su uso exclusivo para la prestación del servicio y en los horarios establecidos.

Anexo N° 15
Matriz de Requisitos Normativos y Contractuales Relacionados a Seguridad de la Información

N°	Normativa o Contrato						Requisito	Proceso involucrado	Sistema de Información involucrado
	Código / referencia	Tipo (*)	Descripción	Entidad u organismo de procedencia (para normativa) / Contraparte (para contrato)	Fecha de inicio de vigencia	Fecha de fin de vigencia			
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

(*) Tipo: Normativa, Contrato