MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA COMISIÓN NACIONAL PARA EL DESARROLLO Y VIDA SIN DROGAS-DEVIDA

DEVIDA
V° B°
Firma Digital

Firmado digitalmente por:
VILLANUEVA DE LOS SANTOS Elvis
Eduardo FAU 20339267821 soft
Motivo: En señal de conformidad
Fecha: 12/02/2025 13:01:54-0500

INDICE

1. FINALIDAD 4

2. BASE LEGAL 4

3. ALCANCE 4

4. **DEFINICIONES** 4

5. FASES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 5

5.1 CONTEXTO DE LA ORGANIZACIÓN 5

5.1.1 Comprensión de organización 5

5.1.2 Comprensión de las necesidades y expectativas de las partes interesadas 5

5.1.3 Determinación del alcance 6

5.1.4 Sistema de gestión de seguridad de la información 6

5.2 LIDERAZGO 6

5.2.1 Liderazgo y compromiso 6

5.2.2 Política y objetivos de Seguridad de la Información 7

5.2.3 Roles, responsabilidades y autoridades organizacionales 7

5.3 PLANIFICACIÓN 8

5.3.1 Gestión de riesgos y oportunidades 8

5.3.2 Declaración de aplicabilidad 8

5.3.3 Objetivos de seguridad de la información 8

5.3.4 Planificación de los cambios 9

5.4 APOYO 9

5.4.1 Recursos 9

5.4.2 Competencias 10

5.4.3 Concientización y capacitación 10

5.4.4 Comunicación 11

5.4.5 Gestión documental del SGSI 11

5.5 OPERACIÓN DEL SGSI 11

5.5.1 Planificación y control operacional 11

El Oficial de Seguridad y Confianza Digital 11

5.5.2 Evaluación de riesgos y oportunidades de seguridad de la información 12

5.5.3 Tratamiento de riesgos y oportunidades de seguridad de la información 12

5.5.4 Identificación, análisis y evaluación de activos de información 12

5.6 EVALUACIÓN DEL DESEMPEÑO 13

5.6.1 Seguimiento, medición, análisis y evaluación del SGSI 13

5.6.2 Auditoría interna al SGSI 14

5.6.3 Revisión por el Comité de Gobierno y Transformación Digital 16

5.7 MEJORA 18

5.7.1 Mejora continua 18

5.7.2 Acciones correctivas y/o de mejoras 18

6 ANEXOS 19

1. FINALIDAD

Normar las fases del Sistema de Gestión de la Seguridad de la Información (SGSI), conforme a lo establecido por la Norma Técnica Peruana *"NTP ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistema de gestión de seguridad de la información. Requisitos. 3ª Edición",* que contribuirán a organizar de manera práctica y eficiente sus fases.

2. BASE LEGAL

2.1 Decreto Legislativo N° 824, Ley de Lucha contra el tráfico ilícito de drogas y sus modificatorias.
2.2 Decreto Supremo N° 047-2014-PCM, que aprueba el Reglamento de Organización y Funciones (ROF) de DEVIDA.
2.3 Resolución de Contraloría N° 146-2019-CG, que aprueba la Directiva N° 006-2019-CG/INTEG "Implementación del Sistema de Control Interno en las Entidades del Estado"; modificada con Resolución de Contraloría N° 130-2020-CG, Resolución de Contraloría N° 093-2021-CG, Resolución de Contraloría N° 095-2022-CG, Resolución de Contraloría N° 073-2023-CG y Resolución de Contraloría N° 320-2024-CG.
2.4 Resolución Directoral N° 014-2018-INACAL/DN, que aprueba la NTP ISO 31000:2018 "Gestión del riesgo. Directrices 2ª Edición".
2.5 Resolución Directoral N° 022-2022-INACAL/DN, que aprueba la NTP ISO/IEC 27001:2022 "Seguridad de la información y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición", la cual reemplaza a la NTP-ISO/IEC 27001:2014.
2.6 Resolución de Gerencia General N° 000204-2024-DV-GG, que aprueba Lineamiento para la gestión de riesgos de la información y tecnología en la Comisión Nacional para el Desarrollo y Vida sin Drogas – DEVIDA.
2.7 Resolución de Gerencia General N° 000019-2024-DV-GG, que aprueba la Directiva N° 002-2024-DV-GG-OPP "Disposiciones para la formulación, modificación, actualización y aprobación de documentos normativos en la Comisión Nacional para el Desarrollo y Vida sin Drogas -DEVIDA".

3. ALCANCE

Las disposiciones contenidas en el presente Manual son de cumplimiento de las Unidades de Organización de la Comisión Nacional para el Desarrollo y Vida sin Drogas - DEVIDA.

4. DEFINICIONES

- **Acción correctiva (AC):** Acción tomada para eliminar la causa de una No conformidad detectada, con la finalidad de evitar nuevamente su aparición. Le corresponde una Solicitud de Acción Correctiva (SAC).
- **Acción de mejora (AM):** Acción que incrementa la capacidad de la entidad para cumplir los requisitos de la NTP ISO/IEC 27001:2022 y que no actúa sobre problemas reales o potenciales ni sobre sus causas. Le corresponde una Solicitud de Acción de Mejora (SAM).
- **Activo de información:** Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la entidad. Por ejemplo: información física o digital, hardware, software, servicios, etc. Cada activo de información es valorado teniendo en cuenta su importancia en cuanto a su confidencialidad, integridad y disponibilidad.
- **Dueño/a de proceso:** Es la persona responsable de la gestión, control y supervisión de un proceso específico dentro de DEVIDA.

- **Hallazgo:** Es una falla, omisión o situación real o potencial que es detectada y puede constituirse en una No Conformidad, Observación u Oportunidad de Mejora.
- **No conformidad (NC):** Incumplimiento de un requisito de la NTP ISO/IEC 27001:2022 o Anexo A de esta misma norma.
- **Observación (OBS):** Son situaciones que, si no se abordan adecuadamente, podrían convertirse en un riesgo o una no conformidad en el futuro.
- **Oportunidad:** Las oportunidades son las situaciones favorables para la entidad o unidad de organización, que deben ser aprovechadas, previa evaluación, por la entidad pues se tiene cierta certeza de que pueden contribuir al cumplimiento de los objetivos estratégicos o generar beneficios.
- **Oportunidad de mejora (OM):** Son situaciones que evidencian mejora del SGSI, siempre que se estime relevante; se relacionan con el hecho de que a pesar que las actividades del SGSI se estén ejecutando según lo planificado y cumpliendo los requisitos de la NTP ISO/IEC 27001:2022 o Anexo A, se pueden hacer mejoras.
- **Producto:** Bien o servicio que proporciona DEVIDA a una población beneficiaria, ciudadanos u otras entidades con el objeto de satisfacer sus necesidades; adicionalmente también se considera como producto a los activos de información, proyectos de TI, planes, implementaciones de nuevas tecnologías, desarrollo y despliegue de aplicaciones, procesos, entre otros que necesiten una evaluación de riesgos de la información y tecnología.
- **Riesgo:** Es la posibilidad de que un evento o circunstancia imprevista afecte negativamente en la entidad o parte de esta, generando consecuencias adversas en la operación, reputación, finanzas, tecnología o seguridad.

5. FASES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1 CONTEXTO DE LA ORGANIZACIÓN[1]

El Oficial de Seguridad y Confianza Digital tiene la responsabilidad de desarrollar y documentar el contexto de la organización[2] como parte de la implementación y operación del sistema de gestión de seguridad. Esta tarea se enmarca en los numerales 5.1.1, 5.1.2 y 5.1.3 del presente manual, los cuales exigen, respectivamente, la comprensión de la organización, las necesidades y expectativas de las partes interesadas y determinación del alcance del SGSI. Para documentar lo desarrollado se debe emplear el Anexo N° 01: Análisis de contexto y determinación del alcance.

5.1.1 Comprensión de organización

Se debe realizar un análisis exhaustivo para entender el entorno en el que opera la entidad. Asimismo, es crucial identificar las amenazas y oportunidades que puedan influir en la seguridad de la información de la entidad. Comprender el contexto de la entidad proporciona una base sólida para el diseño y desarrollo de políticas, objetivos, y procedimientos orientados a garantizar la seguridad de la información.

5.1.2 Comprensión de las necesidades y expectativas de las partes interesadas

Es fundamental identificar y comprender las necesidades y expectativas de las partes interesadas. Para lograrlo, se deben llevar a cabo las siguientes acciones:

- Determinar las partes interesadas pertinentes al Sistema de Gestión de Seguridad de la Información.
- Los requisitos en seguridad de la información de las partes interesadas.

[1] Conforme al Numeral 4 de la Norma Técnica Peruana ISO/IEC 27001:2022.
[2] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.

- Determinar cuál de los requisitos del punto anterior se abordarán mediante el Sistema de Gestión de Seguridad de la Información.

5.1.3 Determinación del alcance

Tras realizar el análisis del contexto de la entidad, comprensión de las necesidades y expectativas de las partes interesadas, es necesario definir los límites del Sistema de Gestión de la Seguridad de la Información (SGSI), especificando los procesos de las Unidades Organización que estarán cubiertos por este sistema; asimismo, es importante considerar los siguientes aspectos:

- El contexto interno y externo de la entidad.
- Los requisitos de las partes interesadas.
- Las interfaces y dependencias entre actividades realizadas por la entidad u proveedores, otras organizaciones, ciudadanos, etc.

5.1.4 Sistema de gestión de seguridad de la información

DEVIDA debe establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (en adelante SGSI), incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de la Norma Técnica Peruana *"NTP ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistema de gestión de seguridad de la información. Requisitos. 3ª Edición".*

5.2 LIDERAZGO[3]

5.2.1 Liderazgo y compromiso

La Presidencia Ejecutiva y Gerencia General demuestran liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información de la siguiente manera:

- Estableciendo una Política y Objetivos del Sistema de Gestión de Seguridad de la Información alineados a los objetivos estratégicos de la entidad.
- Identificando e incorporando los requisitos de seguridad en los procesos incluidos dentro del alcance del SGSI.
- Estableciendo y asegurando el funcionamiento continuo del Comité de Gobierno y Transformación Digital; además, de otros roles y responsabilidades en el ámbito de la seguridad de la información.
- Incorporando personal altamente calificado o especializado en seguridad de la información.
- Apoyando a otros roles de gestión relevantes para que contribuyan con la eficacia del SGSI.
- Asegurando la disponibilidad de los recursos necesarios para la operación y mantenimiento del SGSI.
- Contratando servicios de auditoría, para identificar las oportunidades de mejora del SGSI.
- Capacitando y concientizando al personal en materia de seguridad de la información, ciberseguridad y protección de datos personales.

[3] Conforme al Numeral 5 de la Norma Técnica Peruana ISO/IEC 27001:2022.

- Comunicando la importancia de una gestión eficaz de la seguridad de la información, así como la necesidad de alinear y cumplir con los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI)
- Dirigiendo y apoyando al personal para contribuir a la efectividad del SGSI.
- Asegurando que el SGSI logre los resultados previstos.
- Fomentando el avance constante en la protección de la información.

5.2.2 Política y objetivos de Seguridad de la Información

El Oficial de Seguridad y Confianza Digital tiene la responsabilidad de desarrollar y documentar la política y objetivos de seguridad de la información[4]; dicha política y los objetivos de seguridad de la información debe reflejar el compromiso de DEVIDA con la protección de los datos y los recursos físicos que los respaldan y fomentar una cultura sólida de seguridad de la información dentro de la Comisión Nacional para el Desarrollo y Vida sin Drogas – DEVIDA; asimismo, debe estar alineada a las normativas aplicables.

La política y los objetivos de seguridad de la información deben:

- Ser compatible con el propósito de la entidad.
- Incluir los objetivos de seguridad de la información, conforme al numeral 5.3.3 del presente manual.
- Incluir el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información.
- Incluir el compromiso de mejora continua del SGSI.
- Estar documentada y ser comunicada las partes interesadas internas y externas.

Además, la entidad debe garantizar que el personal y las personas/empresas que presten servicios, cualquiera sea su condición o modalidad contractual, conozcan y cumplan con la política y los objetivos de seguridad de la información.
El titular de la Comisión Nacional para el Desarrollo y Vida sin Drogas – DEVIDA, es el Presidente Ejecutivo; es responsable de aprobar la política y los objetivos de seguridad de la información en cumplimiento del numeral 4.1 de la Resolución de SGTD N° 003-2023-PCM/SGTD.

Para desarrollar este numeral se debe emplear el Anexo N° 02: Política y objetivos de seguridad de la información.

5.2.3 Roles, responsabilidades y autoridades organizacionales

El Comité de Gobierno y Transformación Digital[5] debe asegurar que las responsabilidades y autoridades para los roles pertinentes a la seguridad la información, estén asignadas y comunicadas dentro de la entidad; debiendo asignar la responsabilidad y la autoridad mínimamente para:

- Asegurar que el Sistema de Gestión de Seguridad de la Información este conforme a los requisitos de la NTP ISO/IEC 27001:2022.
- Informar sobre el desempeño del Sistema de Gestión de Seguridad de la Información a la Alta Dirección.
- Gestionar la implementación, mantenimiento y mejora continua del SGSI.

[4] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
[5] En cumplimiento de la función d) del artículo 2 de la Resolución de Presidencia Ejecutiva N° 047-2019-DV-PE, con fecha 11 de abril de 2019.

También se consideran las normativas a las cuales la entidad está sujeta a cumplimiento, al momento de formular los roles, responsabilidades y autoridades.

Para documentar lo roles y responsabilidades se utiliza el Anexo N° 03: Roles y responsabilidades del SGSI.

Por otro lado, para designar un rol a un personal se emplea el Anexo N° 04: Designación de roles y responsabilidades del SGSI.

5.3 PLANIFICACIÓN[6]

5.3.1 Gestión de riesgos y oportunidades

Las Unidades de Organización bajo el ámbito del SGSI de DEVIDA planifican acciones para abordar riesgos y oportunidades que puedan influir en su/s producto/s. Su objetivo es asegurar los resultados esperados, maximizar los efectos positivos, prevenir o mitigar impactos negativos, y promover la mejora continua.

Para ello, se debe emplear los Lineamientos para la gestión de riesgos de la información y tecnología en la Comisión Nacional para el Desarrollo y Vida sin Drogas – DEVIDA y formatos correspondientes.

5.3.2 Declaración de aplicabilidad

El Oficial de Seguridad y Confianza Digital tiene la responsabilidad de desarrollar y documentar la declaración de aplicabilidad[7], una vez finalizada la gestión de riesgos, se debe elaborar una Declaración de aplicabilidad empleando el Anexo N° 05; documento que lista los controles del Anexo A de la NTP ISO/IEC 27001:2022, los cuales se irán comparando con controles de seguridad seleccionados para mitigar los riesgos previamente identificados como parte del tratamiento de riesgo de la gestión de riesgos y los controles generales existentes dentro del alcance del SGSI, identificando de esta manera su aplicabilidad, redactando la justificación de la inclusión o exclusión.

5.3.3 Objetivos de seguridad de la información

El Oficial de Seguridad y Confianza Digital tiene la responsabilidad de[8] formular objetivos de seguridad de la información que cumplan con:

- Ser coherentes con la política general de seguridad de la información.
- Ser medible, de ser posible.
- Se debe tomar en cuenta requisitos aplicables de seguridad de la información y resultados de la evaluación y tratamiento de riesgos.
- Ser objeto de seguimiento
- Ser comunicados
- Actualizarse según corresponda
- Estar disponible como información documentada

Los objetivos deben actualizarse según corresponda y estar disponibles como información documentada en el Anexo N° 02 y Anexo N° 06 del presente manual. Para lograr los objetivos de

[6] Conforme al Numeral 6 de la Norma Técnica Peruana ISO/IEC 27001:2022.
[7] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
[8] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.

seguridad de la información, se debe realizar una planificación previa, la cual cumple con lo siguiente:

- Que se hará
- Que recursos serán requeridos
- Quien será el responsable
- Cuando se culminará
- Como los resultados serán evaluados

Los resultados obtenidos de la definición de los objetivos y su planificación para alcanzarlos deben registrarse en el Anexo N° 06: Planificación y monitoreo de objetivos del SGSI.

5.3.4 Planificación de los cambios

Cuando se presentan cambios internos o externos que afecten al SGSI o seguridad de la información, el Oficial de Seguridad y Confianza Digital debe determinan las acciones a tomar según la magnitud del cambio[9], las cuales se llevarán a cabo de manera planificada y controlada, empleando el Anexo N° 07: Planificación de cambios. Asimismo, el Oficial de Seguridad y Confianza Digital puede solicitar apoyo en el registro de la ficha a las Unidades Organización pertinentes.

5.4 APOYO[10]

5.4.1 Recursos

Para asegurar la operación, mantenimiento y mejora continua del SGSI, el Comité de Gobierno y Transformación Digital[11] debe asegurar mediante las gestiones necesarias que se dispongan y otorguen los recursos suficientes a fin de garantizar el correcto funcionamiento del SGSI. Estos recursos deben estar reflejados en los presupuestos asignados.

Además, si como resultado de la evaluación de riesgos y oportunidades se requiere la implementación de un plan de acción[12], la Alta Dirección debe garantizar la disponibilidad de los recursos necesarios para su correcta ejecución.

A continuación, se presenta los diferentes tipos de recursos requeridos para operar, mantener y mejorar eficazmente el SGSI.

- **Servicios contratados:** Servicios de capacitaciones al personal, auditorías externas, consultorías especializadas, mantenimiento de sistemas de seguridad, seguros contra riesgos de seguridad de la información, contingencias y crisis, entre otros.
- **Recursos humanos:** Personal especializado en seguridad de la información, como un Oficial de Seguridad y Confianza Digital o un equipo de profesionales en seguridad informática. También incluye recursos para la formación y capacitación continua del personal en temas de seguridad, así como para la concienciación y sensibilización sobre la importancia de la seguridad de la información.
- **Recursos informáticos y/o tecnológicos:** Infraestructura de hardware y software, como servidores, dispositivos de red, firewalls, sistemas de detección y prevención de

[9] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
[10] Conforme al Numeral 7 de la Norma Técnica Peruana ISO/IEC 27001:2022.
[11] En cumplimiento de la función d) del artículo 2 de la Resolución de Presidencia Ejecutiva N° 047-2019-DV-PE, con fecha 11 de abril de 2019.
[12] Para este propósito se debe emplear el Lineamiento para la gestión de riesgos de la información y tecnología en la Comisión Nacional para el Desarrollo y Vida sin Drogas – DEVIDA, aprobado mediante Resolución de Gerencia General N° 204-2024-DV-GG con fecha 4 de diciembre de 2024.

intrusiones (IDS/IPS), sistemas de gestión de eventos de seguridad (SIEM), herramientas de cifrado, software antivirus, entre otros.

- **Otros recursos:** Son las normativas adquiridas como la NTP ISO/IEC 27001, 27002, entre otras; asimismo, abarca la infraestructura física adecuada para albergar los equipos de TI y los datos de la entidad de manera segura, incluyendo centros de datos, salas de servidores, sistemas de climatización, sistemas de energía ininterrumpida (UPS), sistemas de extinción de incendios, sistemas de seguridad física, entre otros.

Para registrar los recursos se emplea el Anexo N° 08: Recursos asignados al SGSI.

5.4.2 Competencias

La Alta Dirección, junto con las partes que considere necesarias, determina las competencias requeridas para el personal de la entidad, que cuyas actividades puedan afectar la seguridad de la información, basándose en su nivel educativo, formación o experiencia relevante; dichas competencias deben figurar en el Manual de Perfiles de Puestos[13] (MPP). Además, se debe garantizar que el personal remita la documentación que evidencie de manera objetiva el cumplimiento de dichas competencias, la cual es conservada en su expediente personal o legajo.

Cuando el personal no cuente con todas las competencias requeridas y cuando la entidad considere conveniente capacitar a su personal, estas capacitaciones se podrán planificar mediante los programas que se hayan contemplado para la concientización o capacitación del personal, como lo es el Plan de concientización y capacitación del SGSI (Anexo N° 10)

Asimismo, periódicamente se debe realizar una evaluación de competencias que comprenda tanto las relacionadas a su cargo, como también en materia de seguridad de la información, para lo cual se emplea el Anexo N° 09: Evaluación de competencias; y almacenando las evidencias de la evaluación.

5.4.3 Concientización y capacitación

Para fomentar el compromiso de todo el personal con los aspectos relacionados con el SGSI, es fundamental promover una cultura enfocada en la confidencialidad, integridad y disponibilidad de la información. Además, se debe concientizar sobre la importancia de gestionar adecuadamente los riesgos y aprovechar las oportunidades.

El Oficial de Seguridad y Confianza Digital debe asegurar que el personal tome conciencia y éste capacitado sobre:

- La Política y Objetivos de Seguridad de la Información.
- Las Directivas o Lineamientos en materia de seguridad de la información, ciberseguridad y protección de datos personales en el contexto de la entidad.
- Su contribución a la eficacia del SGSI.
- Los beneficios de un mejor desempeño de la seguridad de la información.
- Las consecuencias de no cumplir con los requisitos del SGSI.
- Las amenazas cibernéticas actuales.
- Otros que sean necesarias para la seguridad de la información.

Asimismo, el Oficial de Seguridad y Confianza Digital puede apoyarse en las Unidades Organización pertinentes para la ejecución de las actividades de concientización y capacitación.

[13] Aprobado mediante Resolución de Gerencia General N° 156-2019-DV-GG y sus modificatorias; Resolución de Gerencia General N° 164-2019-DV-GG, Resolución de Gerencia General N° 0098-2021-DV-GG, Resolución de Gerencia General N° 000102- 2021-DV-GG, Resolución de Gerencia General N° 000207-2022-DV-GG, Resolución de Gerencia General N° 000228-2023-DV-GG y Resolución de la Unidad de Recursos Humanos N° 076-2024-DV-OGA-URH.

Las actividades de concientización y capacitación en materia de seguridad de la información, ciberseguridad y protección de datos personales se registran empleando el Anexo N° 10: Plan de concientización y capacitación del SGSI.

5.4.4 Comunicación

El Oficial de Seguridad y Confianza Digital tiene la responsabilidad de determinar las necesidades de comunicación tanto internas como externas, referentes al Sistema de Gestión de la Seguridad de la Información (SGSI)[14]; asimismo, debe tener en consideración mínimamente para determinar las comunicaciones lo siguiente:

- Que comunicar
- Cuando comunicar
- Con quien comunicarse
- Como comunicarse

Con el fin de realizar este numeral se emplea el Anexo N° 11: Matriz de comunicaciones.

5.4.5 Gestión documental del SGSI

Se debe definir tanto la información exigida por la NTP ISO/IEC 27001:2022 como aquella que considere esencial para asegurar la eficacia del SGSI. Asimismo, establece los lineamientos para la correcta gestión de los documentos, con el fin de mantener un control adecuado de la estructura documental dentro del SGSI. Este control también abarca los documentos de origen externo, siempre que sea posible, se prioriza el uso de documentación digital, facilitando su acceso y evitando la utilización de documentos desactualizados.

Para ello, emplea los “Lineamientos para la gestión de la información documentada del SGSI” vigente y sus formatos. Además, la Gestión documental del SGSI estará a cargo del Oficial de Seguridad y Confianza Digital[15].

Si bien, el presente manual contempla formatos, no se deben limitar estos; es decir se pueden usar los “Lineamientos para la gestión de la información documentada del SGSI” vigente, para agregar los demás puntos correspondientes a un formato, mas no se puede quitar ningún punto de los formatos del presente manual.

5.5 OPERACIÓN DEL SGSI[16]

5.5.1 Planificación y control operacional

El Oficial de Seguridad y Confianza Digital[17] debe elaborar y ejecutar un programa operacional del SGSI para realizar el seguimiento a la ejecución de los requisitos, y las acciones determinadas en los numerales 5.1, 5.2, 5.3, 5.4, 5.6 y 5.7 del presente manual alineados a las cláusulas de la NTP ISO/IEC 27001:2022, empleando el Anexo N° 12: Programa operacional del SGSI.

Para asegurar que terceros o servicios externos, que son pertinentes para el sistema de gestión de seguridad de la información son controlados, para lo cual se debe contemplar los siguientes controles del Anexo A de la NTP ISO/IEC 27001:2022, dependiendo de su aplicabilidad:

[14] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
[15] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
[16] Conforme al Numeral 8 de la Norma Técnica Peruana ISO/IEC 27001:2022.
[17] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.

- **A 5.20** Abordar la seguridad de la información dentro de los acuerdos con proveedores.
- **A 5.21** Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (TIC).
- **A 5.22** Seguridad de la información en el uso de servicios en la nube.

Asimismo, se debe controlar los cambios planeados y para controlar las consecuencias de los cambios no planificados, actuando para mitigar cualquier efecto adverso al SGSI, según sea necesario, a través del Anexo N° 07: Planificación de los cambios.

5.5.2 Evaluación de riesgos y oportunidades de seguridad de la información

Los responsables de las Unidades Organización y/o Dueños de procesos, en colaboración con el Oficial de Seguridad y Confianza Digital, llevarán a cabo la evaluación de riesgos y oportunidades de seguridad de la información al menos una vez al año, o cuando se produzcan cambios significativos en la entidad o procesos dentro del alcance del SGSI.

La evaluación se realiza conforme el numeral 5.3.1 del presente manual.

5.5.3 Tratamiento de riesgos y oportunidades de seguridad de la información

Los responsables de las Unidades Organización y/o Dueños de procesos, en colaboración con el Oficial de Seguridad y Confianza Digital, deben elaborar y ejecutar un plan de acción para tratar los riesgos identificados como parte de la evaluación de riesgos, conforme a lo definido en el numeral 3 del Lineamiento para la gestión de riesgos de la información y tecnología en la Comisión Nacional para el Desarrollo y Vida sin Drogas – DEVIDA[18] .

La evaluación se realiza conforme el numeral 5.3.1 del presente manual.

5.5.4 Identificación, análisis y evaluación de activos de información

El Oficial de Seguridad y Confianza Digital[19] tiene la responsabilidad, en cooperación con los dueños de procesos y responsables de unidades de organización[20] debe identificar sus activos de información y determinar la importancia para el proceso o la entidad obteniendo así su nivel de importancia. Para identificar los activos de información, propietarios, custodios, entre otros, con el fin de documentar su realización emplean el Anexo N° 13: Inventario de activos de información críticos y deben tener en consideración lo siguiente:

- Se debe identificar el nivel de confidencialidad, integridad y disponibilidad que requiere el activo de información, para lo cual se define:

Tabla N° 1 Criterios de seguridad y sus niveles

	Muy Alto	Alto	Medio	Bajo
	10	8	6	4
Confidencialidad	Activos de información cuya divulgación o fuga tendría consecuencias severas en materia legal, reputacional u operacional.	Activos de información cuya divulgación o fuga tendría una alta consecuencia en materia legal, reputacional u operacional.	Activos de información cuya divulgación o fuga tendría consecuencias moderadas en materia legal, reputacional u operacional.	Activos de información cuya divulgación o fuga tendría consecuencias mínimas o ninguna.

[18] Aprobado con Resolución de Gerencia General N° 204-2024-DV-GG con fecha 04 de diciembre de 2024.
[19] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
[20] Conforme al numeral 4.8 del artículo 4 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que menciona que son responsables de apoyar en la gestión de riesgos, la cual inicia con la identificación, análisis y evaluación de activos.

	Muy Alto	Alto	Medio	Bajo
	10	8	6	4
Integridad	Activos de información cuya alteración comprometería gravemente la operación, reputación o el cumplimiento legal.	Activos de información que, si son alterados, podrían comprometer la funcionalidad de algún sistema, comprometer la operación, reputación o el cumplimiento legal.	Activos de información cuya modificación podría tener un impacto moderado en la operación, entidad, reputación.	Activos de información no críticos cuya modificación accidental o malintencionada no trae consecuencias importantes.
Disponibilidad	Activos de información cuya indisponibilidad tiene un impacto severo, interrumpiendo operaciones esenciales o comprometiendo la seguridad de la información.	Activos de información cuya indisponibilidad interrumpe las operaciones o comprometiendo la seguridad de la información.	Activos de información cuya indisponibilidad impacta moderadamente las operaciones o seguridad de la información.	Activos de información cuya indisponibilidad tiene una afectación baja o nula; es decir sin consecuencias importantes.

- Una vez obtenidos los niveles de confidencialidad, integridad y disponibilidad requeridos por el activo de información, se calcula el nivel de importancia del activo de información, para lo cual se compara el nivel de los criterios y se toma el nivel más alto de estos, el cual se convierte en el "nivel de importancia del activo".

Tabla N° 2 Ejemplo de valoración

Criterios	Nivel	
Confidencialidad	**Alto**	**8**
Integridad	**Bajo**	**4**
Disponibilidad	**Medio**	**6**

El nivel más alto de los criterios es el nivel Alto (8), por lo que este es el nivel de importancia del activo de información.

5.6 EVALUACIÓN DEL DESEMPEÑO[21]

5.6.1 Seguimiento, medición, análisis y evaluación del SGSI

Planificación

a) El Oficial de Seguridad y Confianza Digital[22] tiene la responsabilidad de evaluar el desempeño de la seguridad de la información y la eficacia del SGSI, se establece indicadores para medir los objetivos de seguridad de la información; asimismo, se debe elaborar indicadores para los controles de la declaración de aplicabilidad, considerando que estén implementados y sean críticos; en ambos casos se debe determinar su frecuencia de medición.

b) Para documentar los indicadores y los resultados de su medición se emplea el Anexo N° 06: Planificación y Monitoreo de objetivos del SGSI.

[21] Conforme al Numeral 9 de la Norma Técnica Peruana ISO/IEC 27001:2022.
[22] Conforme al literal a) del artículo 7 de la Directiva N° 001-2023-PCM/SGTD, que establece el Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.

c) Semestralmente el Oficial de Seguridad y Confianza Digital revisa el documento de Planificación y Monitoreo de objetivos del SGSI, con el fin de identificar los indicadores a ser medidos.

Seguimiento y medición

d) El Oficial de Seguridad y Confianza Digital, mide los indicadores de los objetivos y controles de seguridad de la información, según su frecuencia definida en la Planificación y Monitoreo de objetivos del SGSI.

e) Los dueños de los procesos responsables de los indicadores brindan su apoyo entregando la información necesaria para la medición de los indicadores cuando lo requiera el Oficial de Seguridad y Confianza Digital.

Análisis y evaluación

f) En caso el Oficial de Seguridad y Confianza Digital detecte que no se cumple con la meta establecida, debe comunicar a el dueño del proceso para que tome las acciones necesarias y realice las mejoras correspondientes; con plazo máximo hasta la siguiente medición.

g) El Oficial de Seguridad y Confianza Digital es responsable de emitir y remitir el reporte al Comité de Gobierno y Transformación Digital de los resultados del seguimiento, medición, análisis y evaluación del SGSI; previamente deben ser analizados y evaluados empleando el Anexo N° 06: Planificación y Monitoreo de objetivos del SGSI.

5.6.2 Auditoría interna al SGSI

Al menos una vez al año se realiza una auditoría interna al SGSI para mantener su idoneidad, para lo cual se debe realizar primero el Programa de auditoría (Anexo N° 14) para mantener un control y registro de este; asimismo, se tiene en cuenta lo siguiente:

Planificación antes de la ejecución de la auditoría interna

- Las auditorías son realizadas por personal externo o terceros contratados, para lo cual el Oficial de Seguridad y Confianza Digital debe coordinar y enviar el TDR a la Unidad de Abastecimiento con los requisitos que deben cumplir los postulantes.

- Las auditorías pueden ser desarrolladas por un Auditor Líder, es decir sin la participación de un Equipo de Auditores Internos.

- El Equipo Auditor está compuesto por personal debidamente calificado para llevar a cabo la auditoría, y sin ningún vínculo directo con el proceso que se audita; manteniendo así la objetividad e imparcialidad en la auditoría.

- El Equipo Auditor debe cumplir las siguientes funciones y responsabilidades:

Tabla N° 3: Responsabilidades de los miembros del equipo auditor

Miembros	Responsabilidades
Auditor Líder	Dirigir la reunión de apertura y cierre de auditoría.
	Liderar al equipo de auditoría interna.
	Cumplir con los principios de auditoría, que son: integridad, presentación imparcial, debido cuidado profesional, confidencialidad e independencia, enfoque basado en la evidencia.

Miembros	Responsabilidades
	Elaborar y comunicar el plan de auditoría interna a los auditores internos, y velar por su cumplimiento.
	Dedicación exclusiva mientras dura la auditoría interna.
	Cumplir con el plan de auditoría interna
	Asegurarse de la legitimidad de las evidencias recogidas, la confiabilidad de los datos y registros guardando la debida objetividad.
	Elaborar el informe de auditoría interna.
Auditor Interno (integrantes del equipo)	Cumplir los principios de auditoría, que son: integridad, presentación imparcial, debido cuidado profesional, confidencialidad e independencia, enfoque basado en la evidencia.
	Dedicación exclusiva mientras dura la auditoría interna
	Velar por la legitimidad de las evidencias obtenidas procurando la objetividad en la toma de datos y en los muestreos y/o inspecciones realizadas.
	Cumplir con el horario y cronograma detallado según el plan de auditoría interna.
	Seguir las instrucciones específicas del auditor líder respecto al Plan de Auditoría Interna.
	Entregar los hallazgos al auditor líder para la elaboración del informe de auditoría interna.

- El equipo auditor debe cumplir mínimamente el siguiente perfil para poder realizar la auditoría.

Tabla N° 4 Perfil del equipo auditor

	Auditor Líder	Auditor Interno
Educación	Título Profesional Universitario en Ingeniería de Sistemas o carreras vinculadas a la actividad o especialidad.	
Formación	Certificación o curso como Auditor Líder o Interno en la norma ISO/IEC 27001 vigente.	Certificación o curso de interpretación o Auditor Interno en la norma ISO/IEC 27001 vigente.
Experiencia en la especialidad	Mínimo tres (03) auditorías en entidades (privadas y/o públicas) como auditor líder o auditor interno.	Mínimo dos (02) auditorías en entidades (privadas y/o públicas) como auditor líder o auditor interno.

Ejecución de la auditoría interna

- El Auditor Líder o Equipo Auditor debe realizar una reunión de apertura con el Oficial de Seguridad y Confianza Digital, para presentar los objetivos, el alcance y el enfoque de la auditoría, además de discutir aspectos logísticos y resolver cualquier duda sobre el proceso; de ser posible debe estar las demás partes pertinentes a la auditoría interna.
- El Auditor Líder o Equipo Auditor deben elaborar y enviar el Plan de auditoría interna (Anexo N° 15) al Oficial de Seguridad y Confianza Digital y demás partes pertinentes para mantenerlas informadas.
- Los auditados deben dar las facilidades del caso a los auditores a fin de que se cumplan las actividades planificadas para la auditoría.
- En caso de que el Auditor Líder o Equipo Auditor soliciten información, esta se le brinda en conformidad con el "Lineamiento para la clasificación de la información", para mantener la seguridad de la información.

- Si existiera algún cambio durante el proceso de auditoría, el Auditor Líder actualiza el Plan de auditoría interna y se comunica a los involucrados.
- El Auditor Líder o Equipo Auditor, audita los procesos y/o unidades de organización previstas, de acuerdo con el Plan de auditoría interna, recabando la evidencia objetiva que conduce a los hallazgos de la auditoría.
- Los hallazgos que figuran en los informes de auditoría, deben cumplir con lo siguiente:
  - ✓ Los hallazgos de la auditoría se clasifican en No conformidad, Observación y Oportunidad de Mejora
  - ✓ Redactarse de forma objetiva, precisa y útil que sean entendidas fácilmente por el auditado, a fin de que se pueda analizar e implementar acciones correctivas y preventivas a futuro.
  - ✓ La redacción de los hallazgos debe reflejar claramente su naturaleza y tipo (No Conformidad, Observación u Oportunidad de Mejora), utilizando adecuadamente los verbos que indiquen las acciones necesarias para abordar cada situación.
  - ✓ Contar con la evidencia objetiva específica según sea el caso (código y nombre de documento, ubicación, fecha, etc.)
- El Auditor Líder debe redactar el borrador del Informe de auditoría interna (Anexo N° 16) y presentarlo en una reunión a el Oficial de Seguridad y Confianza Digital, para socializarlos y obtener sus observaciones y correcciones necesarias para después elaborar el Informe de auditoría interna final.

Cierre de la auditoría interna

- El Auditor Líder debe actualizar el Informe de auditoría interna según lo acordado en la reunión con el Oficial de Seguridad y Confianza Digital y enviar el Informe de auditoría interna a este, como máximo 3 días hábiles después de finalizada la auditoria.
- El Auditor Líder junto con el Oficial de Seguridad y Confianza Digital debe presenta el Informe de Auditoría Interna final al Comité de Gobierno y Transformación Digital
- El Oficial de Seguridad y Confianza Digital envía el Informe de auditoría Interna a los responsables de las Unidades Organización, de los procesos auditados y demás partes pertinentes.

5.6.3 Revisión por el Comité de Gobierno y Transformación Digital

El Comité de Gobierno y Transformación Digital debe revisar el Sistema de Gestión de Seguridad de la Información, en cumplimiento de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que menciona:

"El Comité de Gobierno y Transformación Digital institucional es responsable de la dirección, mantenimiento y supervisión estratégica de los planes, resultados y recursos del SGSI (…)"

Adicionalmente, cabe mencionar que, el Gerente General, máxima autoridad de la Gerencia General, es quien Preside el Comité de Gobierno y Transformación Digital en representación del Presidente Ejecutivo[23], por lo que se tiene la participación de la Alta Dirección de DEVIDA para la revisión del SGSI. La revisión se realiza mínimamente una vez al año, pudiendo ser después de la auditoría interna o externa del SGSI, para asegurar su idoneidad, operación y eficacia.

[23] En cumplimiento del artículo 1 de la Resolución de Presidencia Ejecutiva N° 047-2019-DV-PE, con fecha 11 de abril de 2019, que menciona "El/la Gerente General en representación del Presidente Ejecutivo de la Comisión Nacional para el Desarrollo y Vida sin Drogas - DEVIDA, quien Preside el Comité; (…)".

Para la revisión se deben seguir las siguientes pautas:

Programación

- El Oficial de Seguridad y Confianza Digital agenda una reunión con el Comité de Gobierno y Transformación Digital para la revisión del SGSI; la modalidad de la reunión puede ser presencial o virtual, según disponibilidad del Comité.

Información para la revisión

- El Oficial de Seguridad y Confianza Digital prepara toda la documentación necesaria del Sistema de Gestión de Seguridad de la Información, teniendo en consideración lo siguiente:
  - ✓ Estado de los acuerdos y/o acciones anteriores.
  - ✓ Cambios en asuntos internos y externos que podrían afectar al SGSI.
  - ✓ Evaluación del desempeño de seguridad de la información.
  - ✓ Estado de los indicadores y metas programadas de los objetivos, procesos y controles.
  - ✓ Resultados de auditorías internas y externas.
  - ✓ Estado de los hallazgos de auditorías y acciones correctivas.
  - ✓ Recomendaciones de mejora (incluidas las recomendaciones de las partes interesadas, si fuera el caso).
  - ✓ Resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgo.
  - ✓ Estado de las oportunidades de mejora y proyectos de mejora relacionados al SGSI (si fuera el caso).
  - ✓ Incidentes de seguridad de la información y aprendizaje de estos.
  - ✓ Otros temas relevantes para el SGSI

Revisión

- El día programado para la revisión, el Oficial de Seguridad y Confianza Digital presenta la documentación al Comité de Gobierno y Transformación Digital, de ser necesario puede apoyarse en otro personal experto, para explicar algunos temas específicos o técnicos fuera de su especialidad.
- El Comité de Gobierno y Transformación Digital en conjunto con el Oficial de Seguridad y Confianza Digital, realizan el análisis y evaluación de la documentación y en base a este análisis, determinan acuerdos, acciones de mejora y cualquier necesidad de cambio para el SGSI.
- Obtenido el resultado, el Ejecutivo de la Unidad de Tecnología de Información y Comunicación registra los resultados de la revisión del SGSI empleando el Acta definida en los “Lineamientos para la gestión de la información documentada del SGSI”, anexando la información relevante de los acuerdos y acciones tomados de mejora para el SGSI y con las firmas de los asistentes.
- En caso queden temas pendientes por revisar se programa una próxima revisión, la cual debe estar registrada en acta.

Comunicación de resultados

- El Oficial de Seguridad y Confianza Digital distribuye a las partes pertinentes, las acciones y acuerdos tomados en la revisión, a través de correo electrónico.
- El Gerente General envía al Presidente Ejecutivo mediante correo electrónico el acta y los resultados de la revisión del SGSI.

5.7 MEJORA[24]

5.7.1 Mejora continua

DEVIDA mejora continuamente la eficacia del SGSI mediante la implementación y cumplimiento de su Política y objetivos de seguridad de la información, medición de los indicadores y corrección de los hallazgos de auditoría.

Cuando los resultados obtenidos no son los esperados y ante cualquier no conformidad, corresponde al Oficial de Seguridad y Confianza Digital en colaboración con las Unidades Organización pertinentes, implementar las acciones correctivas necesarias para eliminar las causas que dieron origen a la no conformidad y se aseguran de implementar los cambios necesarios para evitar que dicha no conformidad vuelva a ocurrir.

5.7.2 Acciones correctivas y/o de mejoras

Identificación de la NC, OBS y OM

El Oficial de Seguridad y Confianza Digital o Responsable de la Unidad de Organización identifican una NC, OBS o OM, bajo los siguientes escenarios:

- ✓ La revisión por el Comité de Gobierno y Transformación Digital.
- ✓ Las auditorías internas o externas.
- ✓ En la gestión de riesgos y oportunidades.
- ✓ En la verificación de las metas establecidas de los indicadores
- ✓ En la verificación sobre el cumplimiento de los requisitos legales y otros específicos que se apliquen a los procesos del SGSI.
- ✓ Incidentes de seguridad de la información.
- ✓ Análisis de la documentación.
- ✓ Revisión de controles aplicados.
- ✓ Los reclamos de los clientes que se repiten y proceden.
- ✓ Observaciones realizadas por el personal.
- ✓ La revisión de las necesidades y expectativas de las partes interesadas.
- ✓ El análisis del contexto.
- ✓ La medición de los indicadores de los objetivos, controles y procesos.
- ✓ La evaluación de registros del SGSI.
- ✓ Las lecciones aprendidas de experiencias pasadas.

Registro de la acción correctiva o de mejora

- El Oficial de Seguridad y Confianza Digital o Responsable de Unidad de Organización registran la Solicitud de acciones correctivas o de mejoras empleando el Anexo N° 17.
- El Oficial de Seguridad y Confianza Digital en conjunto las partes pertinentes realizan el análisis de las causas de la no conformidad, observación y oportunidad de mejora.

[24] Conforme al Numeral 10 de la Norma Técnica Peruana ISO/IEC 27001:2022.

- Se debe proponer acciones adecuadas con las causas identificadas, indicando fechas, responsables y recursos necesarios para las acciones propuestas; se entiende lo mencionado anteriormente como un plan de acción.

Implementación y seguimiento

- El responsable del plan de acción realiza la implementación de sus actividades según cronograma.
- El responsable del plan de acción comunica al Oficial de Seguridad y Confianza Digital el avance o término de las actividades mediante un correo electrónico o reunión.
- El Oficial de Seguridad y Confianza Digital hace el seguimiento al plan de acción mediante el Anexo N° 18 Seguimiento de SAC o SAM.
- Cualquier inconveniente ocurrido durante la ejecución del plan de acción se debe solucionar eficientemente, de manera que no afecte el cronograma o al menos la fecha de término.
- Todo cambio de las fechas del cronograma debe ser actualizado en la Solicitud de acciones correctivas o de mejoras, por el Oficial de Seguridad y Confianza Digital.

Verificación de la eficacia

Al término del plan de acción se debe verificar si realmente es eficaz para levantar la no conformidad u observación; o aprovechar la oportunidad de mejora. Se emplea el Anexo N° 18: Seguimiento de SAC o SAM.

6 ANEXOS

- Anexo N° 01: Análisis de contexto y determinación del alcance.
- Anexo N° 02: Política y objetivos de seguridad de la información.
- Anexo N° 03: Roles y responsabilidades del SGSI.
- Anexo N° 04: Designación de roles y responsabilidades del SGSI.
- Anexo N° 05: Declaración de aplicabilidad.
- Anexo N° 06: Planificación y Monitoreo de objetivos del SGSI.
- Anexo N° 07: Planificación de cambios.
- Anexo N° 08: Recursos asignados al SGSI.
- Anexo N° 09: Evaluación de competencias.
- Anexo N° 10: Plan de concientización y capacitación del SGSI.
- Anexo N° 11: Matriz de comunicaciones.
- Anexo N° 12: Programa operacional del SGSI.
- Anexo N° 13: Inventario de activos de información críticos.
- Anexo N° 14: Programa de auditoría.
- Anexo N° 15: Plan de auditoría interna.
- Anexo N° 16: Informe de auditoría interna.
- Anexo N° 17: Solicitud de acciones correctivas o de mejoras.
- Anexo N° 18: Seguimiento de SAC o SAM.

Anexo N° 01: Análisis de contexto y determinación del alcance

1. **FINALIDAD**
   [Finalidad del presente documento]

2. **BASE LEGAL**
   [Base legal relacionada al documento]

3. **ALCANCE**
   [Alcance del presente documento]

4. **CONTEXTO DE LA ORGANIZACIÓN**

4.1 Entender la organización y su contexto

4.1.1 Análisis del contexto interno

a) Descripción de la entidad
b) Visión
c) Misión
d) Valores
e) Lineamientos
f) Funciones
g) Objetivos Estratégicos institucionales y de gobierno digital
h) Estructura de la organización
i) Servicios Digitales
j) Infraestructura tecnológica
k) Procesos
l) Personal

4.1.2 Análisis del contexto externo

Económico
- Factor N

Social
- Factor N

Tecnológico
- Factor N

Ecológico
- Factor N

Legal
- Factor N

4.1.3 Análisis FODA

a) Factores Internos

FORTALEZAS		DEBILIDADES	
F1	[Redactar fortaleza]	D1	[Redactar debilidad]
F2	[Redactar fortaleza]	D2	[Redactar debilidad]
FN	[Redactar fortaleza]	DN	[Redactar debilidad]

b) Factores Externos

OPORTUNIDADES		AMENAZAS	
O1	[Redactar oportunidad]	A1	[Redactar amenaza]
O2	[Redactar oportunidad]	A2	[Redactar amenaza]
ON	[Redactar oportunidad]	AN	[Redactar amenaza]

4.2 Comprender las necesidades y expectativas de las partes interesadas

4.2.1 Partes interesadas relevantes

Partes interesadas internas

- Parte interesada interna 1…
- Parte interesada interna N…

Partes interesadas externas

- Parte interesada externa 1…
- Parte interesada externa N…

4.2.2 Requisitos de seguridad de las partes interesadas

PARTES INTERESADAS RELEVANTES		CÓDIGO REQUISITO	REQUISITOS RELEVANTES DE SEGURIDAD DE LA INFORMACIÓN
PARTES INTERNAS	Interesado 1	R1	[Redactar el requisito 1]
		R2	[Redactar el requisito 2]
	Interesado 2	R3	[Redactar el requisito 3]
	Interesado 3	R4	[Redactar el requisito 4]
PARTES EXTERNAS	Interesado 4	R5	[Redactar el requisito 5]
	Interesado 5	R6	[Redactar el requisito 6]
		R7	[Redactar el requisito 7]
		RN	[Redactar el requisito N]

4.2.3 Requisitos que abordará el SGSI

[Requisitos escritos por código que serán abordados por el SGSI]

4.3 Determinación del alcance del sistema de gestión de seguridad de la información

4.3.1 Aplicabilidad del SGSI

[Justificación del por qué se aplica el SGSI]

4.3.2 Interfaces y dependencias

[Describir las interacciones y conexiones entre diferentes componentes, sistemas, procesos o partes interesadas que pueden influir en la seguridad de la información.]

4.3.3 Alcance del SGSI

[Detalla los procesos seleccionados para formar parte del alcance del SGSI]

4.4 Límites del alcance

[Describir los límites del alcance de manera precisa dentro de las cuales el **Sistema de Gestión de Seguridad de la Información** (SGSI) opera, estableciendo qué activos, procesos, áreas organizacionales, tecnologías y ubicaciones físicas están cubiertos por este*]*

5. ACTUALIZACIÓN DEL PRESENTE DOCUMENTO

[Definir cuando o en qué casos se actualiza el documento]

Anexo N° 02: Política y objetivos de seguridad de la información política

[Se redacta los compromisos de la Alta Dirección con la seguridad de la información]

OBJETIVOS

[Se define los objetivos de seguridad de la información, que son metas específicas, medibles y alineadas con la política. Estos objetivos guiarán las actividades de seguridad de la información y ayudarán a evaluar el éxito de las medidas implementadas.]

Anexo N° 03: Roles y responsabilidades del SGSI

1. FINALIDAD

[El siguiente párrafo es un ejemplo, este puede modificarse]

Definir de manera precisa los roles y responsabilidades de todas las partes involucradas en la gestión y operación del SGSI, en cumplimiento con el numeral 5.3 de la Norma Técnica Peruana NTP ISO/IEC 27001, así como con lo dispuesto en el artículo 4 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD.

2. BASE LEGAL

[Base legal relacionada al documento]

3. ALCANCE

[El siguiente párrafo es un ejemplo, este puede modificarse]

El presente documento es de cumplimiento obligatorio principalmente para el personal de DEVIDA vinculado al alcance del SGSI o a quienes se les asigne los roles y responsabilidades definidos en el presente documento, independientemente de su régimen laboral o contractual

4. DEFINICIONES

[Redactar las definiciones de las palabras técnicas, para que el lector tenga un mejor y rápido entendimiento del documento]

5. ESTRUCTURA ORGANIZACIONAL DEL SGSI

[Definir la estructura organizacional del SGSI por medio de un gráfico]

6. ROLES Y RESPONSABILIDADES

[Definir los roles y responsabilidades del SGSI considerando normativas externas o indicaciones internas de las Unidades Orgánicas]

7. ASIGNACIÓN Y COMUNICACIÓN DE LOS ROLES Y RESPONSABILIDADES

[Definir la manera de la comunicación de los roles y responsabilidades del SGSI asignados]

8. ACTUALIZACIÓN DEL PRESENTE DOCUMENTO

[Definir cuándo o en qué casos se actualiza el documento]

Anexo N° 04: Designación de roles y responsabilidades del SGSI.

FECHA: *[DD/MM/AAAA]*	**HORA:** *[HH:MM]*
NOMBRES Y APELLIDOS: *[Nombre del servidor a quien se le designa el cargo]*	
Estimado/a *[Nombre del servidor]*, Por medio de la presente, en el marco del establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), se le comunica que, en adición a sus funciones desempeñará un rol fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información. A continuación, se detalla el rol asignado y las responsabilidades asociadas: **Rol:** *[Nombre del rol asignado].* **Descripción del rol:** *[Breve descripción del rol].* **Fecha de inicio:** *[Fecha de inicio de la asignación del rol].* **Documento de referencia:** *[Ley, Norma, Resolución, Acta, etc.]*	
RESPONSABILIDADES	
• *[Responsabilidad 1]* • *[Responsabilidad 2]* • *[Responsabilidad 3]* • ...	
CONSIDERACIONES	
Su desempeño en este rol será de vital importancia para el éxito de nuestro SGSI. Confiamos en sus habilidades y conocimientos para cumplir con las responsabilidades asignadas de manera efectiva y contribuir con la seguridad de la información en nuestra entidad. Es importante que conozca y comprenda las políticas, procedimientos y controles establecidos en el marco del SGSI relacionados con el rol designado.	
FIRMA DEL PRESIDENTE DE COMITÉ	**FIRMA DEL SERVIDOR DESIGNADO**
[Nombres y apellidos]	**[Nombres y apellidos]**

Anexo N° 05: Declaración de aplicabilidad

Registrado por:	**Fecha de registro:**

CONTROLES ORGANIZACIONALES			
NUMERAL	**CONTROL NTP ISO/IEC 27001:2022**	**APLICA**	**JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN**
CONTROLES PERSONALES			
NUMERAL	**CONTROL NTP ISO/IEC 27001:2022**	**APLICA**	**JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN**
CONTROLES FISICOS			
NUMERAL	**CONTROL NTP ISO/IEC 27001:2022**	**APLICA**	**JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN**
CONTROLES TECNOLÓGICOS			
NUMERAL	**CONTROL NTP ISO/IEC 27001:2022**	**APLICA**	**JUSTIFICACIÓN DE LA INCLUSIÓN O EXCLUSIÓN**

Anexo N° 06: Planificación y monitoreo de objetivos del SGSI

Registrado por:	**Fecha de registro:**

PLANIFICACIÓN PARA ALCANZAR LOS OBJETIVOS									
N°	**Objetivos de seguridad de la información**	**Objetivos específicos de seguridad de la información**	**Acciones**	**Recursos Necesarios**	**Responsable**	**Ejecutor**	**Fecha de Finalización**	**Evaluación de los Resultados**	**Fuente de Información**

MONITOREO DE LOS OBJETIVOS							
N°	**Objetivos de seguridad de la información**	**Objetivos específicos de seguridad de la información**	**Indicador**	**Fórmula**	**Frecuencia de Evaluación**	**Mes**	**Meta**

FICHA DE MEDICIÓN DE INDICADORES								**GRAFICOS DE ANÁLISIS**	**RESULTADO**
Objetivo	**Indicador**	**Métricas**	**Fórmula**	**Métricas**		**Total**	**Meta**		
				A	**B**				

Anexo N° 07: Planificación de cambios.

IDENTIFICACIÓN DEL CAMBIO							
Responsable de la planificación							
ORIGEN DEL CAMBIO (Marca con una X)							
Cambio en la normatividad		**Modificaciones en contexto interno o externo**		**Necesidades y/o expectativas de las partes interesadas**		**Actualización de la NTP ISO/IEC 27001**	
Cambios en la estructura organizacional		**Cambios en los procesos**		**Cambios en el producto/servicio**		**Cambio en la infraestructura tecnológica**	
Disponibilidad de recursos		**Otro (cual)**					

ANÁLISIS DEL CAMBIO	
DESCRIPCIÓN	
PROPÓSITO	
CONSECUENCIAS O EFECTOS POTENCIALES	
PROCESOS AFECTADOS POR EL CAMBIO	

EQUIPO DE TRABAJO PARA EL CAMBIO			
N°	**NOMBRE**	**CARGO**	**UNIDAD DE ORGANIZACIÓN**

ACEPTACIÓN DEL CAMBIO		
¿SE ACEPTA?		**JUSTIFICACIÓN**
SI		
NO		

PLANIFICACIÓN DEL CAMBIO			
Preguntas sobre el cambio a realizar	**SI**	**NO**	**JUSTIFICACIÓN**
¿El cambio implica modificaciones en la planeación estratégica?			
¿Es necesario modificar la política y/o los objetivos de seguridad de la información?			
¿Es necesario modificar el mapa de procesos?			
¿Es necesario modificar el objetivo o alcance de algún proceso?			
¿Es necesario modificar las actividades, las secuencias o las interacciones de algún proceso?			
¿Es necesario ajustar los parámetros de control o mecanismo de seguimiento, medición, análisis y evaluación de algún proceso?			
¿Es necesario contratar externamente algún servicio y/o adquirir un bien?			
¿Es necesario programar capacitación/es para el personal involucrado?			
¿Se requiere actualizar la matriz de evaluación de riesgos e identificar nuevos controles?			

¿Se requiere actualizar o cambiar los controles de seguridad existentes?			

RECURSOS NECESARIOS			
N°	**Descripción del recurso**	**Costo**	**Fecha de adquisición / contrato**

RIESGOS ASOCIADOS AL CAMBIO (usar Guía metodología para la gestión de riesgos y oportunidades)					
Descripción del riesgo	**Probabilidad**	**Impacto**	**Nivel de exposición**	**Controles actuales**	**¿Necesita tratamiento?**

OPORTUNIDADES ASOCIADAS AL CAMBIO (usar Guía metodología para la gestión de riesgos y oportunidades)					
Descripción de la oportunidad	**Probabilidad**	**Impacto**	**Nivel de exposición**	**Controles actuales**	**¿Se aprovechará?**

HOJA DE RUTA				
N°	**Actividades / Acciones**	**Responsable**	**Fecha inicio**	**Fecha fin**

SEGUIMIENTO DEL CAMBIO (durante y después del cambio)			
N°	**Fecha**	**Responsable**	**Resultado**

CONCLUSIÓN DE LA GESTIÓN DEL CAMBIO		
Fecha	**Estado**	**Observaciones**

_____

[Nombres y Apellidos]
[Cargo del responsable de la planificación]

Anexo N° 08: Recursos asignados al SGSI

Registro por :	**Fecha de registro:**

RECURSOS HUMANOS						
N°	**Cargo**	**Funciones**	**Responsable de supervisión**	**Fecha de contratación**	**Fecha de termino**	**Sueldo mensual**
PRESUPUESTO TOTAL PARA LOS RECURSOS HUMANOS						**S/ -**

RECURSOS INFORMÁTICOS Y/O TECNOLÓGICOS						
N°	**N° de Compra**	**Detalle**	**Responsable**	**Fecha de adquisición**	**Fecha de baja**	**Costo total**
PRESUPUESTO TOTAL PARA LOS RECURSOS INFORMÁTICOS Y/O TECNOLÓGICOS						**S/ -**

SERVICIOS CONTRATADOS						
N°	**N° de Servicio**	**Detalle**	**Responsable**	**Fecha de inicio del servicio**	**Fecha de fin de servicio**	**Costo total**
PRESUPUESTO TOTAL PARA LOS SERVICIOS CONTRATADOS						**S/ -**

OTROS RECURSOS					
N°	**Recurso**	**Descripción**	**Responsable / Propietario**	**Fecha de adquisición**	**Costo total**
PRESUPUESTO TOTAL PARA OTROS RECURSOS					**S/ -**

PRESUPUESTO TOTAL	**S/ -**

Anexo N° 09: Evaluación de competencias

Registrado por:	**Fecha de registro:**

INFORMACIÓN PERSONAL			
NOMBRES Y APELLIDOS			
N° DE DNI			
CORREO ELECTRÓNICO			
GRADO ACADEMICO			
INFORMACIÓN LABORAL			
CARGO EN DEVIDA		**RÉGIMEN LABORAL**	
ROL DEL SGSI		**FECHA DE INGRESO**	

EVALUACIÓN DE COMPETENCIAS				
COMPETENCIAS		**EVIDENCIA**	**CUMPLE COMPETENCIA**	**CUMPLIMIENTO DEL PERFIL**
Seguridad				
Cargo				

RECOMENDACIONES		
RECOMENDACIÓN	**POSIBLE FECHA DE EJECUCIÓN**	**ESTADO**

Anexo N° 10: Plan de concientización y capacitación del SGSI

Registrado por :	**Fecha de registro:**

PLANIFICACIÓN																		**Estado de ejecución**
N°	**Concientización / Capacitación**	**Dirigido a**	**Responsable**	**Modalidad**	**Periodicidad**	**Período [AÑO]**												
						Ene	**Feb**	**Mar**	**Abr**	**May**	**Jun**	**Jul**	**Ago**	**Set**	**Oct**	**Nov**	**Dic**	

Anexo N° 11: Matriz de comunicaciones

Registrado por:	**Fecha de Registro:**

N°	QUÉ COMUNICAR	QUIÉN DEBE COMUNICAR	A QUIÉN COMUNICAR	CUANDO COMUNICAR	CANAL DE COMUNICACIÓN	PERÍODO [AÑO]											
						ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SET	OCT	NOV	DIC
COMUNICACIÓN INTERNA																	
COMUNICACIÓN EXTERNA																	

Anexo N° 12: Programa operacional del SGSI

Registrado por:	**Fecha de registro:**

Responsable	**Objetivo**
	Monitorear la adecuada implementación de los planes, programas y actividades establecidos para garantizar la eficiencia del Sistema de Gestión de Seguridad de la Información (SGSI), tomando acciones correctivas cuando surjan imprevistos o desviaciones.

N°	**Actividades**	**Periodo [AÑO]**												**Estado**	**Observaciones**
		Ene	**Feb**	**Mar**	**Abr**	**May**	**Jun**	**Jul**	**Ago**	**Set**	**Oct**	**Nov**	**Dic**		

Anexo N° 13: Inventario de activos de información críticos

Registrado por:	**Fecha de registro:**

Registrado por:				**Fecha de registro:**								
Código	**Nombre del activo**	**Detalle activo**	**Tipo**	**Ubicación**	**Unidad de Organización**	**Propietario del activo**	**Custodio del activo**	**Clasificación**	**Criterios de seguridad**			**Nivel de importancia del activo**
									Confidencialidad	**Integridad**	**Disponibilidad**	

Anexo N° 14: Programa de auditoría

Registrado por:	**Fecha de registro:**

OBJETIVOS DEL PROGRAMA	**CRITERIOS / NORMAS A SER UTILIZADOS**

CRONOGRAMA DE AUDITORÍAS

N°	**Descripción de la auditoría**	**Proceso/Unidad de Organización**	**Periodo [AÑO]**												**Estado**	**Observación**
			Ene	**Feb**	**Mar**	**Abr**	**May**	**Jun**	**Jul**	**Ago**	**Set**	**Oct**	**Nov**	**Dic**		

Anexo N° 15: Plan de auditoría interna.

DATOS GENERALES			
Auditoría Interna Nº		**Fecha de Ejecución**	
Objetivo			
Alcance			
Criterios de la Auditoría			
Lugar de la Auditoría			

EQUIPO AUDITOR		
Nombres y Apellidos	**Rol**	**Siglas**

CRONOGRAMA

N°	**Fecha**	**Horario**	**Siglas de auditor**	**Requisitos**	**Auditado**

Firma en señal de conformidad:

_____

[Nombres y Apellidos]
[Cargo o Rol]

Anexo N° 16: Informe de auditoría interna.

DATOS GENERALES			
N° de auditoría		**Fecha de Auditoría**	
Lugar de auditoría			
OBJETIVO DE LA AUDITORÍA INTERNA			
ALCANCE DE LA AUDITORÍA INTERNA			
EQUIPO AUDITOR			
Nombres y Apellidos	**Rol**		**Siglas**
CANTIDAD DE HALLAZGOS			
No conformidades - NC		**Oportunidades de mejora – OM**	
Observaciones - OB			

DESCRIPCIÓN DE LOS HALLAZGOS				
N°	**Hallazgo**	**Requisito / Control afectado**	**Tipo**	**Comentario**
CONCLUSIONES DE LA AUDITORÍA INTERNA				
RECOMENDACIONES				

_____

[Nombres y Apellidos]
Auditor Líder

Anexo N° 17: Solicitud de acciones correctivas o de mejoras.

ORIGEN DE LA ACCIÓN CORRECTIVA O DE MEJORA (Marca X)		
1	Revisión por la Alta Dirección o Gerencia General	
2	Medición de los indicadores de los objetivos de seguridad de la información	
3	Gestión de riesgos y oportunidades	
4	Revisión de las necesidades y expectativas de las partes interesadas	
5	Auditoría interna	
6	Auditoría externa	
7	Incidente de seguridad de la información	
8	Otro (describa)	

TIPO DE ACCIÓN		**CLASIFICACIÓN DE HALLAZGOS**	
Acción Correctiva (AC)		**No conformidad (NC)**	
Mejora (AM)		**Observaciones (OBS)**	
		Oportunidad Mejora (OM)	
PROCESO INVOLUCRADO		**DUEÑO DEL PROCESO**	

HALLAZGO			
Descripción			
Identificado por	**Fecha**	**Normativa Incumplida**	**Cláusula**

ANÁLISIS DE CAUSAS
ACCIONES INMEDIATAS O CORRECCIÓN:
ANÁLISIS DE RIESGOS

ACCIONES REQUERIDAS	**RESPONSABLE**	**FECHA DE INICIO Y FECHA DE CIERRE**

CONFORMIDAD DE LAS ACCIONES	
[Firma del Presidente del Comité]	**[Firma del dueño del proceso afectado]**
[Nombres y Apellidos] **Presidente del Comité de Gobierno y Transformación Digital**	**[Nombres y Apellidos]** **[Cargo o Rol]**

Anexo N° 18: Seguimiento de SAC O SAM

Registrado por :	**Fecha de Registro:**

Nº de RAC/RAM	**Origen de hallazgo**	**Dueño del proceso afectado**	Descripción hallazgo	Clasificación de hallazgo	Requisito afectado	PLAN DE ACCIÓN				SEGUIMIENTO			VERIFICACIÓN DE LA EFICACIA			**¿Hallazgo levantado?**
						Acciones requeridas	Responsable de las acciones requeridas	Fecha de inicio	Fecha de fin	Fecha de seguimiento	Responsable del seguimiento	Resultados del seguimiento	Fecha de verificación	Responsable de verificación	**Resultados de la verificación**	