

Resolución de Gerencia General

Nº 037-2018-BNP-GG

Lima, 28 DIC. 2018

VISTOS: los Informes Técnicos N° 007-2018-BNP/GG-OSI, N° 012-2018-BNP-GG-OSI y N° 019-2018-BNP-GG-OSI, de fechas 12, 28 de setiembre y 24 de octubre de 2018, de la Oficina de Seguridad de la Información; el Informe Técnico N° 001-2018-BNP-GG-OPP-EMO, el Memorando N° 809-2018-BNP-GG-OPP y el correo electrónico, de fechas 06 de noviembre y 07 de diciembre de 2018, del Equipo de Trabajo de Modernización y de la Oficina de Planeamiento y Presupuesto; el Informe N° 515-2018-BNP-GG-OA-ERH, el Memorando N° 1684-2018-BNP-GG-OA y el correo electrónico, de fechas 15 y 23 de noviembre y 06 de diciembre de 2018, del Equipo de Trabajo de Recursos Humanos y de la Oficina de Administración; y, los Informes Legales N° 281-2018-BNP-GG-OAJ y N° 297-2018-BNP-GG-OAJ de fechas 12 y 26 de diciembre de 2018, de la Oficina de Asesoría Jurídica, y;

CONSIDERANDO:

Que, el artículo 1 de la Resolución Ministerial N° 004-2016-PCM 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;

Que, el numeral 4.4 de la mencionada Norma Técnica Peruana señala respecto del sistema de gestión de seguridad de la información, lo siguiente:

"4.4 Sistema de gestión de seguridad de la información

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, en conformidad con los requisitos de esta Norma Técnica Peruana."

Que, en atención a lo expuesto en el considerando precedente, a través de los Informes Técnicos N° 007-2018-BNP/GG-OSI, N° 012-2018-BNP-GG-OSI y N° 019-2018-BNP-GG-OSI, de fechas 12, 28 de setiembre y 24 de octubre de 2018, la Oficina de Seguridad de la Información presentó la propuesta de Manual de Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú, indicando lo siguiente: "(...) se propone el manual del sistema de gestión de seguridad de la información que nos brinda los lineamientos para realizar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Biblioteca Nacional del Perú. Desde la



Resolución de Gerencia General N° 037 -2018-BNP-GG

determinación del alcance del SGSI hasta la mejora continua del respectivo sistema de gestión”;

Que, mediante Informe Técnico N° 001-2018-BNP-GG-OPP-EMO, Memorando N° 809-2018-BNP-GG-OPP y correo electrónico, de fechas 06 de noviembre y 07 de diciembre de 2018, el Equipo de Trabajo de Modernización y la Oficina de Planeamiento y Presupuesto, emitieron opinión favorable respecto de la mencionada propuesta;

Que, asimismo, a través del correo electrónico de fecha 06 de diciembre de 2018, el Equipo de Trabajo de Recursos Humanos de la Oficina de Administración emitió opinión favorable respecto de la propuesta;

Que, mediante Resolución de Gerencia General N° 025-2018-BNP/GG de fecha 14 de noviembre de 2018, se aprobó el Procedimiento de control de información documentada del Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú;

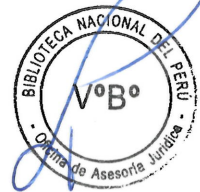
Que, a través de la Resolución de Gerencia General N° 035-2018-BNP-GG de fecha 19 de diciembre de 2018 se modificó el Anexo 01 del Procedimiento de control de información documentada del Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú, referido al nivel de elaboración, revisión y aprobación de documentos internos, indicándose la competencia de la Gerencia General para aprobar manuales referidos al Sistema de Gestión de Seguridad de la Información;

Que, con los Informes Legales N° 281-2018-BNP-GG-OAJ y N° 297-2018-BNP-GG-OAJ de fechas 12 y 26 de diciembre de 2018, la Oficina de Asesoría Jurídica considera que resulta legalmente viable aprobar la referida propuesta;

Con el visado de la Oficial de Seguridad de la Información, del Equipo de Trabajo de Modernización de la Oficina de Planeamiento y Presupuesto, de la Oficina de Planeamiento y Presupuesto, del Equipo de Trabajo de Recursos Humanos de la Oficina de Administración, de la Oficina de Administración; y, de la Oficina de Asesoría Jurídica;

De conformidad con lo dispuesto en la 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; el Reglamento de Organización y Funciones de la Biblioteca Nacional del Perú, aprobado por Decreto Supremo N° 001-2018-MC; y, demás normas pertinentes;





Resolución de Gerencia General N° 037 -2018-BNP-GG

SE RESUELVE:

Artículo 1.- APROBAR el Manual de Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú, que como Anexo forma parte integrante de la presente Resolución.

Artículo 2.- ENCARGAR a la Oficina de Tecnologías de la Información y Estadística la publicación de la presente Resolución en el portal web institucional (www.bnp.gob.pe).

Regístrese y comuníquese.

EMMA ANA MARÍA LEÓN VELARDE AMÉZCAGA
Gerenta General
Biblioteca Nacional del Perú





PERÚ Ministerio de Cultura

Biblioteca Nacional del Perú



MANUAL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código: SGSI-MA-01

Versión: 01




HOJA DE CONTROL DE CAMBIOS DEL DOCUMENTO

Nro. de Cambio	Fecha de Cambio	Tipo ¹	Descripción del cambio	Responsable de modificación



¹ A: Agregar; M: Modificar; E: Eliminar

 biblioteca nacional del peru	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	3 de 18

ÍNDICE


1. OBJETIVO.....	4
2. ALCANCE	4
3. BASE NORMATIVA.....	4
4. DEFINICIONES Y ABREVIATURAS.....	4
5. CONTENIDO.....	6
5.1. CONTEXTO DE LA ENTIDAD.....	6
5.1.1. DETERMINACIÓN DEL ALCANCE DEL SGSI.....	6
5.1.2. REQUISITOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	6
5.2. LIDERAZGO	6
5.2.1. COMPROMISO DE LA ALTA DIRECCIÓN	6
5.2.2. ENUNCIADO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA BIBLIOTECA NACIONAL DEL PERÚ	7
5.2.3. RESPONSABILIDADES EN EL SGSI	7
5.3. PLANIFICACIÓN	10
5.3.1. ACCIONES PARA TRATAR LOS RIESGOS Y LAS OPORTUNIDADES	10
5.3.2. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN	10
5.4. SOPORTE.....	11
5.4.1. RECURSOS	11
5.4.2. CAPACITACIÓN, CONOCIMIENTO Y CAPACIDAD	11
5.4.3. COMUNICACIÓN INTERNA	11
5.4.4. INFORMACIÓN DOCUMENTADA.....	11
5.5. OPERACION.....	13
5.6. EVALUACION DEL DESEMPEÑO	13
5.6.1. MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN.....	13
5.6.2. AUDITORÍA, MEDICIÓN Y MEJORA.....	14
5.6.3. REVISIÓN POR LA ALTA DIRECCIÓN.....	14
5.7. MEJORAS	15
6. REGISTROS	16
7. ANEXOS.....	16



Formato: Digital

La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.

Clasificación: Uso Interno

 biblioteca nacional del Perú	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	4 de 18

1. OBJETIVO

Definir los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información, según la Norma Técnica Peruana vigente en Seguridad de la Información para la Biblioteca Nacional del Perú.

2. ALCANCE

Es aplicable a todo proceso de la Biblioteca Nacional del Perú que es parte del Sistema de Gestión de Seguridad de la Información – SGSI.


3. BASE NORMATIVA

- 3.1. Ley N° 30570, Ley General de la Biblioteca Nacional del Perú.
- 3.2. Ley N° 29733, Ley de Protección de Datos Personales.
- 3.3. Ley N° 27815, Ley del Código de Ética de la Función Pública.
- 3.4. Decreto Supremo N° 001-2018-MC que aprueba el Reglamento de Organización y Funciones de la Biblioteca Nacional del Perú.
- 3.5. Decreto Supremo N° 010-2017-MC que aprueba el Reglamento de la Ley N° 30570, Ley General de la Biblioteca Nacional del Perú.
- 3.6. Decreto Supremo N° 033-2015-PCM que aprueba el Reglamento de la Ley del Código de Ética de la Función Pública.
- 3.7. Decreto Supremo N° 003-2013-JUS que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
- 3.8. 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. 2da. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

4. DEFINICIONES Y ABREVIATURAS

- 4.1. **Acción correctiva:** Acción para eliminar la causa de una No Conformidad y para prevenir la recurrencia.
- 4.2. **Aceptación del riesgo:** Decisión informada para aceptar un riesgo particular.
- 4.3. **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la entidad.
- 4.4. **Alcance:** Ámbito de la entidad que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la entidad.
- 4.5. **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo, y para determinar el nivel de riesgo.
- 4.6. **Autenticación:** Provisión de seguridad de que una característica alegada de una entidad es correcta.
- 4.7. **Confidencialidad:** Propiedad que la información no esté disponible o se da a conocer a personas no autorizadas, entidades o procesos.
- 4.8. **Custodio de activo de información:** Identifica al órgano que tiene la responsabilidad de mantener los niveles de protección adecuados en base a las especificaciones dadas por el propietario del activo de información.
- 4.9. **Declaración de aplicabilidad:** (Statement of Applicability; SoA). Documento que enumera los controles aplicados por el SGSI de la entidad -tras el resultado de los procesos de


Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
------------------	---	----------------------------

 biblioteca nacional del Perú	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	5 de 18

- evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la Norma Técnica Peruana vigente.
- 4.10. **Disponibilidad:** Propiedad de ser accesible y utilizable a petición por una entidad autorizada.
 - 4.11. **Evaluación de riesgos:** Proceso de la comparación de los resultados del análisis de riesgos con criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
 - 4.12. **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una entidad con respecto al riesgo.
 - 4.13. **Identificación de riesgos:** Proceso de encontrar, reconocer y describir los riesgos.
 - 4.14. **Integridad:** Propiedad que busca garantizar una información exacta y libre de errores, la misma que puede ser modificada bajo autorización.
 - 4.15. **Inventario de activos de información:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la entidad, entre los principales) dentro del alcance del SGSI, que tengan valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos.
 - 4.16. **Mejora continua:** Actividad recurrente para mejorar el rendimiento.
 - 4.17. **Nivel de riesgo:** Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad. [Fuente: Guía ISO 73:2009, modificado - "o combinación de riesgos", ha sido suprimido].
 - 4.18. **No conformidad:** (NC): Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.
 - 4.19. **No repudio:** Capacidad para demostrar la ocurrencia de un evento o acción que se atribuye y sus entidades de origen.
 - 4.20. **Parte interesada:** Persona u organización que puede afectar, ser afectado por, o que crean que están afectadas por una decisión o actividad.
 - 4.21. **Plan de tratamiento de riesgos:** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
 - 4.22. **Política de seguridad:** Documento que establece el compromiso de la Alta Dirección y el enfoque de la entidad en la gestión de la seguridad de la información. Según la ISO/IEC 27002, es la intención y dirección general expresada formalmente por la Alta Dirección.
 - 4.23. **Procedimiento:** Forma especificada para llevar a cabo una actividad o un proceso.
 - 4.24. **Proceso de gestión de riesgos:** La aplicación sistemática de políticas, procedimientos y prácticas para las actividades de comunicación, consultoría, estableciendo el contexto y la identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgo.
 - 4.25. **Propietario de activo de información:** Identifica al órgano que tiene responsabilidad aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
 - 4.26. **Registro:** Documento que presenta resultados obtenidos o proporciona evidencias de actividades desempeñadas.
 - 4.27. **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Efecto de la incertidumbre en los objetivos.
 - 4.28. **Riesgo de seguridad de la información:** Posibilidad que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la Biblioteca Nacional del Perú.



Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
------------------	---	----------------------------

 biblioteca nacional del Perú	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	6 de 18

- 4.29. **Seguridad de la información:** La preservación de la confidencialidad, integridad y disponibilidad de la información.
- 4.30. **Sistema de gestión:** Conjunto de elementos interrelacionados o que interactúan de una entidad para establecer políticas, objetivos y procesos para alcanzar dichos objetivos.
- 4.31. **Usuario/a:** Es quien independientemente del régimen laboral o modalidad contractual se vincula a la entidad.
- 4.32. **BNP:** Biblioteca Nacional del Perú.
- 4.33. **SGSI:** Sistema de Gestión de la Seguridad de la Información. Es la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).

5. CONTENIDO

5.1. CONTEXTO DE LA ENTIDAD

5.1.1. Determinación del alcance del SGSI

El alcance debe considerar lo siguiente:

- Aspectos externos e internos de la entidad relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados del SGSI.
- Las partes interesadas y los requisitos concernientes a las partes interesadas relevantes al SGSI (pueden incluir además requisitos legales, regulatorios y obligaciones contractuales).
- Las interfaces y dependencias entre actividades realizadas por la entidad y las que son realizadas por otras entidades.
- Documentar el alcance con los datos anteriormente citados, de acuerdo al Formato para la Determinación del Alcance del SGSI de la BNP.

5.1.2. Requisitos del SGSI

La BNP detalla en el presente documento como se establece, implementa, opera, mantiene y mejora continuamente la eficacia del SGSI, el cual se encuentra documentado de acuerdo con los requisitos de la normativa vigente.


5.2. LIDERAZGO

5.2.1. Compromiso de la Alta Dirección

La Alta Dirección de la BNP busca cumplir la normatividad de seguridad de la información asumiendo el compromiso con el SGSI de:

- Aprobar la política y objetivos de seguridad de la información.
- Comunicar a los/as usuarios/as de la BNP la importancia de satisfacer los requisitos vigentes y reglamentarios aplicables.

Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
-------------------------	---	-----------------------------------

	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	7 de 18

5.2.2. Enunciado de la política de seguridad de la información de la BNP

La BNP, como organismo público ejecutor, con autonomía económica, administrativa y financiera, adscrito al Ministerio de Cultura y, como ente rector del Sistema Nacional de Bibliotecas, reconoce a la información como un activo de vital importancia para el cumplimiento de los objetivos estratégicos institucionales buscando el aseguramiento de la calidad de los servicios para el uso y acceso del material bibliográfico documental a favor de la población, promoviendo el desarrollo humano y la inclusión social.

Marco de referencia para fijar objetivos de seguridad de la información

Garantizar que todos los riesgos de seguridad para la información de la entidad, y la información que otros le confían, se identifiquen, analicen y gestionen para que se mantengan en niveles aceptables. Por lo cual se declaran los siguientes lineamientos:

- Identificar los activos de información que son críticos o sensibles y clasificarlos según disposiciones establecidas para el inventario, tratamiento de activos de información del SGSI.
- Gestionar los riesgos relevantes de seguridad de la información, según disposiciones establecidas para la identificación, análisis y evaluación de riesgos del SGSI.
- Aplicar controles de seguridad de información apropiados para reducir los riesgos a un nivel aceptable. Los controles se describirán en estándares, procedimientos y pautas de seguridad de la información.

Compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información

La BNP garantiza que se aplique un nivel apropiado de seguridad para proteger la confidencialidad, integridad y disponibilidad de su información y que cumpla con los requisitos legales, regulatorios y contractuales aplicables a la seguridad de la información, sobre la base de nuestros valores de excelencia, colaboración, diversidad, integridad, innovación, inclusión y compromiso social, dentro del marco normativo vigente en el Perú.


Compromiso de mejora continua del SGSI

Garantizar la provisión de recursos para mejorar continuamente el SGSI, incluidos los procesos, las técnicas y los controles de seguridad de la información en la BNP.

5.2.3. Responsabilidades en el SGSI

El SGSI de la BNP está conformado por el Comité de Gestión de Seguridad de la Información, los propietarios y custodios de activos de la información, los responsables de los órganos y los/as usuarios/as de la BNP, quienes tienen las siguientes responsabilidades:

Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
-------------------------	---	-----------------------------------

 biblioteca nacional del Perú	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	8 de 18

a. Comité de Gestión de Seguridad de la Información

El Comité de Gestión de Seguridad de la Información debe estar conformado por:

- El/La Titular de la entidad o su representante.
- El/La Gerente/a General.
- El/La Jefe/a de la Oficina de Administración.
- El/La Jefe/a de la Oficina de Planeamiento y Presupuesto.
- El/La Jefe/a de la Oficina de Tecnologías de la Información y Estadística.
- El/La Jefe/a de la Oficina de Asesoría Jurídica.
- El/La Oficial de Seguridad de la Información.



El Comité debe ser presidido por el/la titular de la entidad. Para las reuniones del Comité, no es necesario que se encuentren presentes todos/as los/as integrantes, se debe contar con un mínimo de cuatro (4) integrantes y siempre será necesaria la presencia de un representante del/de la titular de la entidad. En ausencia del presidente del Comité, este debe ser presidido por quien él haya designado. La frecuencia de reuniones del Comité es dos (2) veces al año.



El/La Oficial de Seguridad de la Información es el/la responsable de convocar a las reuniones del Comité de Gestión de Seguridad de la Información y es el/la responsable de llevar el control de las actas de reunión del Comité de Gestión de Seguridad de la Información.



Se podrá requerir la asistencia de otro/a usuario/a de la BNP o consultor externo, cuyo aporte se estime necesario para la correcta toma de decisiones técnicas específicas. Estos miembros sólo tendrán derecho a voz, más no para la votación.

Este Comité es responsable de:

- Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información.
- Promover y gestionar la implementación del SGSI.
- Promover la gestión de seguridad de la información en los procesos y cultura de la entidad.
- Gestionar la asignación del personal y recursos necesarios para la implementación del SGSI.
- Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, en conformidad con los requisitos del SGSI.
- Evaluar el desempeño del SGSI.
- Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.




Oficial de Seguridad de la Información

Es responsable de:



Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
------------------	---	----------------------------

	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	9 de 18

- Elaborar manuales, procedimientos y otra documentación relativa a seguridad de la información según la Norma Técnica Peruana vigente en Seguridad de la Información.
- Proponer y coordinar la gestión de riesgos de los activos de información.
- Supervisar el cumplimiento e implementación de los lineamientos, y procedimientos y/o controles referidos a la seguridad de la información.
- Monitorear cambios significativos en la infraestructura que puedan poner en riesgo los activos de información de la BNP.
- Monitorear la efectividad y eficiencia de los controles implementados para la protección de los activos de información.
- Realizar el mantenimiento del SGSI.
- Gestionar el control de los documentos del SGSI.
- Gestionar las auditorías internas del SGSI.
- Hacer seguimiento de las acciones correctivas y preventivas.
- Apoyar en la revisión por la Alta Dirección del SGSI.
- Promover y hacer seguimiento de la mejora continua del SGSI.
- Informar formalmente al Comité de Gestión de Seguridad de la Información cualquier incidente o exposición de seguridad de la información que represente un riesgo.
- Promover la difusión de una cultura en seguridad de la información al interior de la BNP.
- Ser parte de la implementación y pruebas de los planes de contingencia.
- Otros que considere necesario el Comité de Gestión de Seguridad de la Información.



c. Propietarios de activo de la información

Son responsables de:

- Definir el criterio de clasificación de la información de acuerdo a los niveles de clasificación detallado en el Procedimiento de Inventario, Etiquetado y Tratamiento de Activos de Información.
- Determinar los niveles de acceso que podrán tener los/as usuarios/as sobre la información.
- Autorizar a los/as usuarios/as, la asignación de accesos sobre la información.
- Definir criterios en torno al activo de información respecto a su creación, acceso, modificación y eliminación.
- Definir controles, en coordinación con el/la Oficial de Seguridad de la Información, para la protección de los activos y asegurar su implementación.
- Revisar periódicamente los accesos y privilegios otorgados sobre la información.




d. Custodios de activos de la información

Son responsables de:

- Asignar los niveles de protección adecuados de acuerdo a las especificaciones otorgadas por el propietario del activo de información.
- Resguardar la información siguiendo los lineamientos definidos por el propietario del activo de información para su respectiva protección.



Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
-------------------------	---	-----------------------------------

 biblioteca nacional del Perú	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	10 de 18

e. Responsables de los órganos de la BNP

Deben:

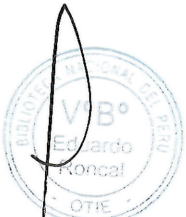
- Asegurar que el personal bajo su cargo conozca y practique los lineamientos y normas de seguridad de la información.
- Asegurar que la información y recursos bajo su control estén debidamente protegidos por las medidas de seguridad adecuadas.
- Asegurarse en reconocer a los propietarios de los activos de información dentro del órgano a su cargo.
- Asegurarse que el personal a su cargo tiene acceso solo a las aplicaciones y datos necesarios para realizar sus tareas.
- Reportar inmediatamente el incumplimiento o infracciones a los lineamientos y normas de seguridad de la información.



Usuarios/as de la BNP

Son responsables de:

- Hacer uso de la información sobre la cual se les ha concedido acceso, solo para fines autorizados.
- Cumplir con las medidas de seguridad establecidas en los lineamientos, normas y procedimientos de seguridad de la información.
- Reportar inmediatamente cualquier incumplimiento de los lineamientos y normas y procedimientos de seguridad de la información.
- Hacer uso de los sistemas de información y la red informática solo para propósitos autorizados e inherentes a la función asignada.
- Cumplir con las actividades definidas en el Procedimiento de Inventario, Etiquetado y Tratamiento de Activos de Información.



5.3. PLANIFICACIÓN

5.3.1. Acciones para tratar los riesgos y las oportunidades

- Desarrollar el plan de tratamiento de riesgos que contenga las opciones para identificar y evaluar las opciones para el tratamiento de riesgos y los criterios de aceptación de los riesgos, así como también los controles que se aplicarán a cada uno de los riesgos.
- La implementación de controles es coordinada por el/la Oficial de Seguridad de la Información y se realiza según el plan de tratamiento de riesgos.



Objetivos de seguridad de la información

Los objetivos de seguridad de la información de la BNP son:


- Garantizar la continuidad del servicio mediante la prevención, el control y la minimización del impacto de los incidentes de seguridad de la información.



Formato: Digital

La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.

Clasificación: Uso Interno

 biblioteca nacional del Perú	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	11 de 18

- Garantizar la confidencialidad, integridad y disponibilidad de la información de la BNP al documentar, implementar y medir los controles de seguridad de la información de acuerdo a las políticas definidas.
- Garantizar que los órganos de la BNP cumplan con los requisitos legales, regulatorios y contractuales con respecto a la seguridad de la información.

5.4. SOPORTE

5.4.1. Recursos



- La BNP elabora una vez al año el presupuesto inicial de apertura, en el que considera los recursos requeridos para la ejecución de los procesos internos, así como la partida referente a los recursos para implementar y mantener el SGSI, mejorar continuamente su eficacia y aumentar la satisfacción de los/as usuarios/as, entre otros.
- Dicho presupuesto es elaborado por la Gerencia General.

5.4.2. Capacitación, conocimiento y capacidad



- Uno de los elementos básicos para el éxito de un SGSI es el recurso humano, por tal motivo se capacita a todo el personal de la BNP que tenga acceso a los sistemas o información.
- Al responsable que administra o gestiona el SGSI se le brinda entrenamiento especializado de acuerdo a sus funciones y responsabilidades.
- Todas las charlas, talleres o entrenamiento en temas de seguridad de la información deben ser registrados por el/la Oficial de Seguridad de la Información.
- La responsabilidad de la ejecución de estas actividades está a cargo del Equipo de Trabajo de Recursos Humanos de la Oficina de Administración y el/la Oficial de Seguridad de la Información.

5.4.3. Comunicación interna

Para la comunicación interna entre los diferentes órganos de la BNP respecto del SGSI y su eficacia, la entidad establece sus comunicaciones internas mediante diferentes mecanismos, los cuales se describen a continuación:

- Charlas en temas de seguridad de la información.
- Reuniones del Comité de Gestión de Seguridad de la Información.
- Reunión con la Alta Dirección.
- Reuniones con los diferentes órganos de la BNP.
- Comunicación a través de la intranet, correo institucional, etc.


5.4.4. Información documentada

a. Requisitos de documentación

La BNP debe contar con documentación que describe el SGSI, los cuales se mencionan a continuación:



Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
-------------------------	---	-----------------------------------

 biblioteca nacional del Perú	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	12 de 18

- Enunciados documentados de la política y objetivos del SGSI.
- Manual del SGSI.
- Manual de Políticas de Seguridad de la Información.
- Procedimiento de inventario, etiquetado y tratamiento de activos de información del SGSI.
- Metodología para la identificación, análisis y evaluación de riesgos del SGSI.
- Plan de tratamiento del riesgo.
- Procedimientos documentados para asegurar la planeación, operación y control de sus procesos de seguridad de la información.
- Procedimientos y controles de soporte.
- Métricas para medir la efectividad de los controles.
- Registros que proporcionan evidencia de las actividades desempeñadas.
- Declaración de aplicabilidad.

Los documentos del SGSI se presentarán en forma impresa o medios electrónicos además de jerarquizados y clasificados según la estructura general que se muestra en la siguiente tabla:

Tabla 01: Estructura de la documentación del SGSI en la BNP

Nivel 1:	Documentación: Políticas, Objetivos
Nivel 2:	Documentación: Manuales, Procedimientos.
Nivel 3:	Documentación: Instructivos y Formatos.
Nivel 4:	Documentación: Registros y documentos externos que tengan relación con el SGSI.


b. Control de documentos

Para controlar los documentos necesarios para la gestión del SGSI, la BNP ha definido que:

- Los documentos son elaborados siguiendo la estructura de documentos definida por la BNP.
- Los documentos son revisados, actualizados cuando es necesario y aprobados nuevamente.
- Los documentos son aprobados para verificar su adecuación, antes de su puesta en circulación.
- Los documentos son identificados con el estado de revisión actualizado.
- Las versiones apropiadas de los documentos están disponibles en las localizaciones donde se lleva a cabo las actividades esenciales para el funcionamiento efectivo del SGSI.
- Los documentos obsoletos se retiran de todos los puntos de publicación y utilización, para evitar su uso no intencional.
- Cualquier documento obsoleto que se conserve por razones legales o referenciales del conocimiento es identificado adecuadamente.
- Los documentos de origen externo son identificados y su distribución se realiza cuando la BNP lo considera necesario.



Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
-------------------------	---	-----------------------------------

 biblioteca nacional del Perú	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	13 de 18

Para este fin, se debe establecer el Procedimiento Control de la Información Documentada, el Formato lista maestra de documentos internos y el Formato lista maestra de documentos externos del SGSI.

c. Control de Registros

Los registros de la BNP son controlados y conservados. Solo aquellos que se requieran para demostrar la conformidad con los requisitos y el funcionamiento efectivo del SGSI, para ello se ha establecido y mantiene un procedimiento documentado.

La identificación, archivo, protección, tiempo de conservación y destino final de los registros se realiza de acuerdo al Procedimiento Control de la Información Documentada, y el Formato lista maestra de registros internos y externos.

Para el control de aquellos registros que se encuentran en medios magnéticos, se aplicará el Procedimiento de respaldo y recuperación de la información.

5.5. OPERACIÓN

5.5.1. Gestión de riesgos de seguridad de la información

La BNP debe contar con la documentación para el inventario y la gestión de riesgos de activos de información del SGSI, la cual es detallada en el Procedimiento de inventario, etiquetado y tratamiento de activos de información del SGSI y la Metodología para la identificación, análisis y evaluación de riesgos del SGSI, los cuales incluyen:

- La identificación de los activos de información que están dentro del alcance del SGSI.
- La identificación de los riesgos.
- El análisis y evaluación de los riesgos.
- Identificación y evaluación de las opciones para el tratamiento de riesgos.
- Selección de controles.
- El resultado de la identificación, análisis, evaluación y el tratamiento de riesgos, son aprobados por el Comité de Gestión de Seguridad de la Información, quienes posteriormente autorizan la implementación y operación del SGSI.
- La declaración de aplicabilidad es desarrollada por el/la Oficial de Seguridad de la Información y es actualizada conforme se realice el análisis de riesgo.
- El análisis de riesgo se realiza una vez al año o cuando ocurra algún cambio en el proceso y/o activos de información que son parte del SGSI.
- En base a los documentos aplicados se deben obtener los siguientes documentos:
 - Inventario de Activos de Información.
 - Análisis y Evaluación de Riesgos.
 - Plan de Tratamiento de Riesgos.
 - Aceptación de Riesgos.
 - Declaración de Aplicabilidad.

5.6. EVALUACIÓN DEL DESEMPEÑO


5.6.1. Monitoreo, medición, análisis y evaluación

Formato: Digital

La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.

Clasificación: Uso Interno



 biblioteca nacional del peru	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	14 de 18

- Evaluar y medir el nivel de desempeño del proceso y reportar los resultados a la Alta Dirección para su revisión.
- Revisar el nivel de riesgo residual y riesgo aceptable identificado, considerando cambios en la entidad, cambios en la tecnología, cambios en los objetivos estratégicos de la BNP, cambios en las amenazas, cambios en el ambiente legal (regulaciones, leyes, etc.).
- Realizar auditorías internas por lo menos una vez al año y guardar evidencia de la revisión.
- Realizar revisiones del SGSI, por parte de la Alta Dirección.
- Mantener registros de las acciones y eventos que puedan impactar al SGSI.



5.6.2. Auditoría, medición y mejora

La BNP debe planear e implantar los procesos de auditoría, revisión y mejora necesarios.

- Para asegurar la conformidad y eficacia del SGSI.
- Para mejorar continuamente la eficacia del SGSI.

a. Auditorías internas del SGSI


La BNP debe realizar anualmente auditorías internas del SGSI para determinar que:

- Está conforme con las actividades planificadas con los requisitos del marco normativo vigente y con los requisitos del SGSI establecidos por la BNP.
- Se ha implantado y se mantiene de manera eficaz para alcanzar los objetivos del SGSI.
- Para la planificación de las auditorías, la BNP determina el Programa de Auditorías Internas del SGSI, las auditorías son planificadas en función al estado e importancia de las actividades, órganos de la BNP, y a los resultados de las auditorías internas realizadas.
- Además, incluye los criterios para la preparación, ejecución, frecuencia y la metodología aplicada incluyendo la selección de auditores. A fin de asegurar la imparcialidad de las mismas se describe en el Procedimiento Auditoría Interna.
- La BNP mantiene registros de los resultados de las auditorías realizadas. Los responsables de los órganos que son auditados se aseguren que se tomen las acciones sin demora para eliminar no conformidades detectadas y sus causas. Las actividades de seguimiento incluyen la verificación de la ejecución de las acciones tomadas y la verificación de la eficacia de las mismas.
- La BNP mantiene registros que indican la naturaleza de las no conformidades y de cualquier acción tomada posteriormente, incluyendo las concesiones que se hayan obtenido.
- Cuando se corrige una no conformidad, ésta es sometida a una nueva verificación para demostrar su conformidad con los requisitos.
- Cuando se detecta una no conformidad después de la entrega de los resultados obtenidos en la auditoría interna, la BNP adopta las acciones apropiadas respecto de las consecuencias, o efectos potenciales, de la no conformidad, tal como se indica en el Procedimiento Gestión de la Mejora Continua del SGSI.



5.6.3. Revisión por la Alta Dirección

Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
-------------------------	---	-----------------------------------

 biblioteca nacional del peru	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	15 de 18

- a. La Alta Dirección efectúa por lo menos una vez al año la revisión del SGSI, con la finalidad de asegurar su continua conformidad, adecuación y eficiencia, así como, evaluar la necesidad de realizar cambios en el SGSI de la entidad, incluyendo la política y los objetivos específicos.
- b. Para la revisión del SGSI, el/la Oficial de Seguridad de la Información debe convocar a una reunión al Comité de Gestión de Seguridad de la Información.



- c. En base a la información enviada por el/la Oficial de Seguridad de la Información, el Comité de Gestión de Seguridad de la Información prepara el informe para la revisión del SGSI.

- d. La revisión periódica incluye la verificación del funcionamiento actual y las oportunidades de mejora asociadas a:



- Evaluación de objetivos y metas programadas.
- Estado de los proyectos relacionados al SGSI.
- Resultados de auditorías y revisiones del SGSI.
- Retroalimentación de las partes interesadas.
- Información sobre el estado de acciones preventivas y correctivas.
- Desempeño y conformidad del SGSI (métricas del SGSI).
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la Alta Dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.

- e. El resultado de la revisión por la Alta Dirección incluye cualquier decisión y acción asociadas a:

- Mejora de la eficacia del SGSI y sus procesos.
- Actualización de la evaluación de riesgos y el plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de la entidad, requerimientos de seguridad de la información, procesos de la entidad, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos.
- Mejoramiento de cómo se mide la efectividad de los controles.



Las actas de reuniones constituyen los registros de esta actividad. Dichas actas se desarrollan en el *Formato Acta de Revisión de la Alta Dirección*, y son archivadas por el/la Oficial de Seguridad de la Información.

El Comité de Gestión de Seguridad de la Información realiza un seguimiento de los acuerdos y encargos aprobados y lo comunica a la Alta Dirección.



5.7. MEJORAS


5.7.1. Acciones correctivas



Formato: Digital

La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.

Clasificación: Uso Interno

 biblioteca nacional del peru	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	16 de 18

Tienen como finalidad eliminar las causas de las no conformidades y evitar su repetición. Las acciones correctivas son apropiadas a los efectos de las no conformidades encontradas. Se ha establecido el Procedimiento Gestión de la Mejora Continua del SGSI. En este documento se definen los requisitos para la:

- Revisión de no conformidades.
- Investigación de las causas de la no conformidad.
- Evaluación de la necesidad de adoptar acciones para asegurar que las no conformidades no vuelvan a ocurrir.
- Determinación e implantación de las acciones necesarias.
- Registro de los resultados de las acciones tomadas.
- Revisión de las acciones correctivas tomadas.



5.7.2. Acciones preventivas

Tienen como finalidad prevenir la aparición de no conformidades y evitar su repetición, y que las acciones preventivas tomadas sean apropiadas para los efectos de los problemas potenciales, tal como se indica en el Procedimiento Gestión de la Mejora Continua del SGSI. Dicho documento está dirigido a la:

- Determinación de no conformidades potenciales y sus causas.
- Evaluación de la necesidad de actuar para prevenir la ocurrencia de no conformidades.
- Determinación e implantación de las acciones necesarias.
- Registro de los resultados de las acciones tomadas.
- Revisión de las acciones preventivas tomadas.



5.7.3. Mejora continua

- Tomar las acciones correctivas y preventivas, basadas en los resultados de la revisión de la Alta Dirección, para lograr la mejora continua del SGSI.
- Identificar mejoras en el SGSI, a fin de implementarlas.
- Comunicar los resultados y las acciones a abordar a todas las áreas usuarias involucradas.
- Revisar el SGSI, donde sea necesario implementar las acciones seleccionadas.
- Para este fin, se ha establecido el Procedimiento Gestión de la Mejora Continua del SGSI.

6. REGISTROS


- 6.1. Formato para la determinación del alcance del SGSI de la BNP (SGSI-FO-04).
- 6.2. Formato Acta de Revisión de la Alta Dirección (SGSI-FO-05).

7. ANEXOS

- 7.1. Anexo 01: Formato para la determinación del alcance del SGSI de la BNP.
- 7.2. Anexo 02: Formato Acta de Revisión de la Alta Dirección.



Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
-------------------------	---	-----------------------------------

 biblioteca nacional del Perú	Manual	Código	SGSI-MA-01
	Sistema de Gestión de Seguridad de la Información para la Biblioteca Nacional del Perú	Versión	01
		Página	17 de 18

Anexo 01: Formato para la determinación del alcance del SGSI de la BNP



PERÚ Ministerio de Cultura Biblioteca Nacional del Perú



DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN


Código: SGSI-FO-04

Versión: 01



Formato: Digital	La impresión de este documento constituye una "COPIA NO CONTROLADA" a excepción de que se indique lo contrario.	Clasificación: Uso Interno
-------------------------	---	-----------------------------------

Anexo 02: Formato Acta de Revisión de la Alta Dirección

 biblioteca nacional del peru	FORMATO	Código	SGSI-FO-05
	Acta de Revisión Alta Dirección	Versión	01
		Página	

Acta N°:		Fecha:		
Hora Inicio:		Hora Término:		
Lugar				
1. Asistentes				
N°	Miembro	Cargo	Firma	
2. Invitados				
N°	Nombre	Cargo	Firma	
3. Agenda				
4. Desarrollo				
5. Acuerdos:				
N°	Tema	Acuerdo	Responsable	Fecha de Cumplimiento

