Resolución de Gerencia General

N° 015-2019-BNP-GG

Lima, 11 MAR. 2019

VISTOS:

Los Informes Técnicos N° 008-2018-BNP/GG-OSI y N° 012-2018-BNP-GG-OSI, de fechas 12 y 28 de setiembre de 2018, de la Oficial de Seguridad de la Información; el correo electrónico de fecha 22 de enero de 2019, del Equipo de Trabajo de Recursos Humanos de la Oficina de Administración; el correo electrónico de fecha 23 de enero de 2019, del Equipo de Trabajo de Logística y Control Patrimonial de la Oficina de Administración; el Informe Técnico N° 000003-2019-GG-OTIE-ERCS de fecha 29 de enero de 2019, del Equipo de Trabajo de Redes, Comunicaciones y Soporte Técnico de la Oficina de Tecnologías de la Información y Estadística; el Memorando N° 000047-2019-BNP-GG-OTIE, de fecha 01 de febrero de 2019, de la Oficina de Tecnologías de la Información y Estadística; el Informe Técnico N° 000030-2019-GG-OPP-EMO de fecha 21 de febrero de 2019, del Equipo de Trabajo de Modernización de la Oficina de Planeamiento y Presupuesto; el Memorando N° 000248-2019-BNP-GG-OPP de fecha 21 de febrero de 2019, de la Oficina de Planeamiento y Presupuesto; el Informe Legal N° 000028-2019-BNP-GG-OAJ de fecha 27 de febrero de 2019, 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 Anexo A de la mencionada Norma Técnica Peruana, referido a los objetivos de control y controles de referencia, señala en el numeral A.5.1 de la Tabla A.1, lo siguiente:

A.5 Políticas de seguridad de la información		
A.5.1 Dirección de la gerencia para la seguridad de la información		
Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.		
A.5.1.1	Políticas para la seguridad	*Control*

	de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes.

Que, a través de los Informes Técnicos N° 008-2018-BNP/GG-OSI y N° 012-2018-BNP-GG-OSI, de fechas 12 y 28 de setiembre de 2018, la Oficial de Seguridad de la Información presentó la propuesta de Manual de Políticas de Seguridad de la Información para la Biblioteca Nacional del Perú, indicando que dicho documento *"(...) proporcionará lineamientos de Seguridad de la Información necesarios para implementar los controles establecidos en la Norma Técnica Peruana NTP-IDO/IEC 27001:2014 en la Biblioteca Nacional del Perú, los cuales permitirán alcanzar los objetivos definidos para el Sistema de Gestión de Seguridad de la Información de la Biblioteca Nacional del Perú";*

Que, mediante correos electrónicos de fechas 22 y 23 de enero de 2019, los Equipos de Trabajo de Recursos Humanos y de Logística y Control Patrimonial, ambos de la Oficina de Administración, emitieron su conformidad respecto de la mencionada propuesta;

Que, por medio del Informe Técnico N° 000003-2019-GG-OTIE-ERCS y del Memorando N° 000047-2019-BNP-GG-OTIE, de fechas 29 de enero y 01 de febrero de 2019, el Equipo de Trabajo de Redes, Comunicaciones y Soporte Técnico y la Oficina de Tecnologías de la Información y Estadística emitieron opinión favorable a la referida propuesta;

Que, a través del Informe Técnico N° 000030-2019-GG-OPP-EMO y del Memorando N° 000248-2019-BNP-GG-OPP, ambos de fecha 21 de febrero de 2019, el Equipo de Trabajo de Modernización y la Oficina de Planeamiento y Presupuesto emitieron opinión favorable a dicha propuesta;

Que, mediante Informe Legal N° 000028-2019-BNP-GG-OAJ de fecha 27 de febrero de 2019, la Oficina de Asesoría Jurídica consideró legalmente viable emitir el acto resolutivo que apruebe la mencionada propuesta;

Que, por medio 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, aprobado mediante Resolución de Gerencia General N° 025-2018-BNP/GG, referido al nivel de elaboración, revisión y aprobación de documentos internos, precisándose que la Gerencia General es competente para aprobar manuales referidos al Sistema de Gestión de Seguridad de la Información;

Resolución de Gerencia General Nº 015 -2019-BNP-GG

Que, a través del literal c) del inciso 1.1 del artículo 1 de la Resolución Jefatural N° 063-2018-BNP de fecha 11 de junio de 2018, se delegó al/a la Gerente/a General, la facultad de aprobar todo tipo de disposiciones internas vinculadas a la conducción de la institución;

Con el visado de la Oficial de Seguridad de la Información; del Equipo de Trabajo de Recursos Humanos de la Oficina de Administración; del Equipo de Trabajo de Logística y Control Patrimonial de la Oficina de Administración; del Equipo de Trabajo de Redes, Comunicaciones y Soporte Técnico de la Oficina de Tecnologías de la Información y Estadística; de la Oficina de Tecnologías de la Información y Estadística; del Equipo de Trabajo de Modernización de la Oficina de Planeamiento y Presupuesto; de la Oficina de Planeamiento y Presupuesto; y, de la Oficina de Asesoría Jurídica;

De conformidad con la Ley N° 30570, Ley General de la Biblioteca Nacional del Perú; el Reglamento de Organización y Funciones de la Biblioteca Nacional del Perú, aprobado por Decreto Supremo N° 001-2018-MC; 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; y, demás normas pertinentes;

SE RESUELVE:

Artículo 1.- APROBAR el Manual de Políticas 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 AMEZAGA
Gerenta General
Biblioteca Nacional del Perú

PERÚ | Ministerio de Cultura | Biblioteca Nacional del Perú

MANUAL
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Código: SGSI-MN-02

Versión: 01

BIBLIOTECA NACIONAL DEL PERÚ V°B° Eduardo Roncal OTIE

BIBLIOTECA NACIONAL DEL PERÚ V°B° Augusto Fernandini OPP

BIBLIOTECA NACIONAL DEL PERÚ V°B° Eduardo Ulloa OPP EMO

BIBLIOTECA NACIONAL DEL PERÚ Oficial de Seguridad de la Información

BIBLIOTECA NACIONAL DEL PERÚ V°B° Jefe E.T. Log. y C.P. Oficina de Administración

HOJA DE CONTROL DE CAMBIOS DEL DOCUMENTO

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

BIBLIOTECA NACIONAL DEL PERÚ V°B° Eduardo Roncal OTIE

BIBLIOTECA NACIONAL DEL PERÚ V°B° Augusto Fernandini OPP

BIBLIOTECA NACIONAL DEL PERÚ V°B° Edderdo Ulloa OPP EMO

BIBLIOTECA NACIONAL DEL PERÚ Oficial de Seguridad de la Información

BIBLIOTECA NACIONAL DEL PERÚ V°B° Gerald Benavente A. Jefe E.T. Log. y C.P. Oficina de Administración

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

ÍNDICE

BIBLIOTECA NACIONAL DEL PERÚ V°B° Eduardo Roncal OTIE

BIBLIOTECA NACIONAL DEL PERÚ V°B° Augusto Fernandini OPP

BIBLIOTECA NACIONAL DEL PERÚ V°B° Eduardo Uiloa OPP EMO

BIBLIOTECA NACIONAL DEL PERÚ Oficial de Seguridad de la Información

BIBLIOTECA NACIONAL DEL PERÚ V°B° Gerald Benavente O. Jefe E.T. Log. y C.P. Oficina de Administración

1. OBJETIVO

Dar a conocer las políticas de seguridad de la información para la Biblioteca Nacional del Perú necesarias para implementar los controles establecidos en el Anexo A de la normativa vigente, los cuales permiten alcanzar los objetivos definidos para la seguridad de la información en la entidad.

2. ALCANCE

Este manual aplica a todo proceso que es parte de un Sistema de Gestión de Seguridad de la Información – SGSI.

3. GLOSARIO DE TÉRMINOS

3.1. **Acción correctiva**: Acción para eliminar la causa de una No Conformidad y para prevenir la recurrencia.
3.2. **Activo**: 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. Cualquier elemento que tiene valor para la entidad.
3.3. **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.
3.4. **Ambiente**: Se refiere al ambiente de trabajo apropiado según el caso que se defina.
3.5. **Amenaza**: Posible causa de un incidente no deseado, que puede resultar en daño a un sistema o entidad.
3.6. **Análisis de riesgos**: Proceso para comprender la naturaleza del riesgo, y para determinar el nivel de riesgo.
3.7. **Ataque**: Intento de destruir, exponer, alterar, inutilizar, robar o ganar acceso no autorizado o no hacer uso de un activo autorizado.
3.8. **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva para determinar el grado en que se cumplen los criterios de auditoría.
3.9. **Autenticación**: Provisión de seguridad de que una característica alegada de una entidad es correcta.
3.10. **Confidencialidad**: Propiedad de la información que no está disponible o se da a conocer a personas no autorizadas, entidades o procesos.
3.11. **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida). Medida que modifica el riesgo.
3.12. **Control de acceso**: Se refiere a garantizar que el acceso a los activos está autorizado y restringido en base a los requerimientos de la entidad y de seguridad.
3.13. **Control preventivo**: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
3.14. **Desastre**: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una entidad durante el tiempo suficiente como para verse la misma afectada de manera significativa.
3.15. **Disponibilidad**: Propiedad de ser accesible y utilizable a petición por una entidad autorizada.
3.16. **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.
3.17. **Evento**: Ocurrencia o cambio de un conjunto particular de circunstancias.
3.18. **Eventos de seguridad de la información**: Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible brecha de la política de seguridad de la información o el fallo de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

3.19. **Gestión de incidentes de seguridad de la información**: Procedimientos para la detección, notificación, evaluar, responder a, tratar con, y aprender de los incidentes de seguridad de la información.
3.20. **Gestión de riesgos**: Actividades coordinadas para dirigir y controlar una entidad con respecto al riesgo.
3.21. **Identificación de riesgos**: Proceso de encontrar, reconocer y describir los riesgos.
3.22. **Impacto**: El costo para la entidad de un incidente - de la escala que sea -, que puede o no ser medido en términos estrictamente financieros por ejemplo, pérdida de reputación, implicaciones legales, entre otros.
3.23. **Incidente de seguridad de la información**: Uno o varios eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la entidad y amenazando la seguridad de la información.
3.24. **Infraestructura tecnológica**: Se encuentra integrada por un conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, entre otros), software (sistemas operativos, bases de datos, lenguajes de programación, herramientas de administración, entre otros) y servicios (soporte técnico, seguros, comunicaciones, entre otros) que, en conjunto, dan soporte a las aplicaciones (sistemas informáticos) de una entidad.
3.25. **Integridad**: Propiedad que busca garantizar una información exacta y libre de errores, la misma que puede ser modificada bajo autorización.
3.26. **Inventario de activos**: 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.
3.27. **Instalaciones de procesamiento de información**: Cualquier sistema de procesamiento de la información, servicios o infraestructuras, o la ubicación física donde será alojada.
3.28. **Mejora continua**: Actividad recurrente para mejorar el rendimiento.
3.29. **No repudio**: Capacidad para demostrar la ocurrencia de un evento o acción que se atribuye y sus entidades de origen.
3.30. **Plan de continuidad del negocio:** Orientado a permitir la continuación de las principales funciones de la entidad en el caso de un evento imprevisto que las ponga en peligro.
3.31. **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.
3.32. **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.
3.33. **Prestador/a de servicios:** Es quien brinda servicios a la entidad, sin tener un vínculo laboral con ella.
3.34. **Propietario**: Identifica a la persona que tiene responsabilidad aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
3.35. **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.
3.36. **Segregación de tareas**: Reparto de tareas sensibles entre distintas personas para reducir el riesgo de un mal uso de los sistemas e información deliberado o por negligencia.
3.37. **Seguridad de la información**: La preservación de la confidencialidad, integridad y disponibilidad de la información.
3.38. **Sistema de gestión**: Conjunto de elementos interrelacionados o que interactúan en una entidad para establecer políticas, objetivos y procesos para alcanzar dichos objetivos.
3.39. **Sistema de información**: Aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo de información.
3.40. **Tratamiento de riesgos**: Proceso para modificar el riesgo.
3.41. **Usuario/a**: Es quien tiene un vínculo laboral con la entidad.
3.42. **Vulnerabilidad:** Debilidad de un activo o de control que puede ser explotado por una o más amenazas.
3.43. **BNP:** Biblioteca Nacional del Perú.
3.44. **SGSI**: Sistema de Gestión de la Seguridad de la Información. 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).

3.45. **TI**: Tecnología de la Información.

4. BASE NORMATIVA

4.1. Ley N° 30570, Ley General de la Biblioteca Nacional del Perú.
4.2. Ley N° 30057, Ley del Servicio Civil.
4.3. Ley N° 29733, Ley de Protección de Datos Personales.
4.4. Ley N° 27815, Ley del Código de Ética de la Función Pública.
4.5. Decreto Supremo N° 001-2018-MC que aprueba el Reglamento de Organización y Funciones de la Biblioteca Nacional del Perú.
4.6. Decreto Supremo N° 010-2017-MC que aprueba el Reglamento de la Ley N° 30570, Ley General de la Biblioteca Nacional del Perú.
4.7. Decreto Supremo N° 004-2019-JUS que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
4.8. Decreto Supremo N° 033-2015-PCM que aprueba el Reglamento de la Ley del Código de Ética de la Función Pública.
4.9. Decreto Supremo N° 040-2014-PCM que aprueba el Reglamento General de la Ley N° 30057, Ley del Servicio Civil.
4.10. Decreto Supremo N° 003-2013-JUS que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
4.11. 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.

5. RESPONSABILIDADES

5.1. El Comité de Gestión de Seguridad de la Información: Promover el cumplimiento del presente documento.
5.2. El/La Oficial de Seguridad de la Información: Verificar el cumplimiento del presente documento.

6. CONTENIDO

6.1. Políticas para la seguridad en recursos humanos

6.1.1. Objetivos

- Asegurar que los/as usuarios/as entiendan sus responsabilidades con respecto a la seguridad de la información, y sean capacitados/as en temas de seguridad de la información, especialmente si trabajarán con información confidencial; y, así, reducir el riesgo de hurto y/o mal uso de los activos de información.

- Asegurar que los/as usuarios/as estén conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que estén preparados para cumplir con las políticas de seguridad de la información establecidas por la BNP, así como también reducir el riesgo de hurto o mal uso de las instalaciones.

- Asegurar que los/as usuarios/as cesen o cambien sus funciones o puesto de trabajo, de una forma ordenada para asegurar que la salida de la BNP esté controlada contemplando el retorno de la información, equipos y derechos de acceso que la entidad considere conveniente.

6.1.2. Alcance

Estas políticas deben ser cumplidas por los/as usuarios/as de los distintos órganos de la BNP.

Las políticas cubren todo el proceso de reclutamiento y contratación de un/una usuario/a, así como, el cambio de funciones o puesto de trabajo y cese de labores.

6.1.3. Políticas

a. **Seguridad de la información en las responsabilidades y funciones del SGSI**

Se deben definir las funciones y responsabilidades del SGSI, el cual debe incluir los siguientes requisitos:

- Asegurar que las responsabilidades sean asignadas a los/as usuarios/as para que sean cumplidas.
- Debe proteger los activos de información de accesos no autorizados, modificación, destrucción o interferencia.
- Reportar eventos de seguridad de la información u otro riesgo de seguridad de la información para la BNP.

b. **Seguridad de la información en la selección de personal**

- El Equipo de Trabajo de Recursos Humanos y el Equipo de Trabajo de Logística y Control Patrimonial, ambos equipos de la Oficina de Administración, deben mantener listas de verificación de los/as candidatos/as a usuarios/as, en concordancia con las leyes, regulaciones, ética y requerimientos de la BNP. Dichas listas deben tomar en consideración la privacidad y la protección de los datos del/de la candidata/a a usuario/a y deben incluir, como mínimo, lo siguiente:
  - La disponibilidad de referencias personales.
  - La comprobación de los documentos de identificación, por ejemplo: currículo vitae, certificados académicos y profesionales.
- Cuando el/la candidata/a sea seleccionado/a, la BNP debe realizar una comprobación más detallada a largo plazo si, por sus actividades laborales, debe acceder a información confidencial.

c. **De las declaraciones de confidencialidad**

- Los/as usuarios/as deben firmar términos y condiciones referidos a sus obligaciones y a las obligaciones de la BNP con respecto a la seguridad de la información.
- Los términos y condiciones deben estar alineados a las funciones y responsabilidades del SGSI definidas en el Manual del Sistema de Gestión de Seguridad de la Información. Además, deben establecer lo siguiente:
  - Todos/as los/as usuarios/as a los que se les debe otorgar acceso a la información y a los servicios de tratamiento de información de la BNP deben firmar una declaración de confidencialidad y no divulgación antes de otorgársele dicho acceso. Ver Anexo 01.
  - Las responsabilidades para la clasificación de la información y la gestión de los activos de información de la BNP asociados con los sistemas de

información y los servicios manejados por los/as usuarios/as deben ser definidas según las Políticas para la Gestión de Activos de Información.

- Los términos y condiciones referentes a la seguridad de la información deben estar de acuerdo a la naturaleza y grado de acceso que tendrá el/la usuario/a a los activos de información de la BNP asociados a los sistemas y servicios de tratamiento de información. Según sea el caso, las responsabilidades contenidas en los términos y condiciones deben continuar por un periodo definido después del término de éste.

d. **Durante el empleo**

- Los Equipos de Trabajo de Recursos Humanos y de Logística y Control Patrimonial de la Oficina de Administración, y los propietarios de información deben asegurarse de que los/as usuarios/as:
  - Cuenten con sus funciones y responsabilidades de seguridad de la información antes de otorgar el acceso a información sensible, o a los servicios de tratamiento de información.
  - Se encuentren capacitados/as para cumplir la Política de Seguridad de la Información de la BNP.
  - Alcancen un nivel de conocimiento de seguridad de la información relevante a sus funciones y responsabilidades dentro de la BNP.
  - Acepten los términos y condiciones del empleo, los cuales incluyen la política de seguridad de la información de la BNP y métodos apropiados de trabajo.

e. **Conocimiento, educación y entrenamiento en seguridad de la información**

- Los/as usuarios/as de la BNP deben recibir entrenamiento en seguridad de la información y deben conocer los lineamientos, procedimientos y documentación relacionada a seguridad de la información de la BNP, así como, de la actualización de los mismos, según sea relevante para el desempeño de sus funciones en la BNP.

- El Equipo de Trabajo de Recursos Humanos de la Oficina de Administración conjuntamente con el/la Oficial de Seguridad de la Información deben realizar el entrenamiento en el conocimiento de seguridad de la información, con una inducción formal que incluya el dar a conocer la Política de Seguridad de la Información de la BNP, antes de conceder acceso a la información, servicios de tratamiento de información o iniciar el servicio. El entrenamiento debe incluir también requisitos de seguridad de la información, responsabilidades legales, así como, prácticas en el uso correcto de los servicios de tratamiento de información.

f. **Sobre los procedimientos administrativos disciplinarios**

- Debe evaluarse el inicio de un procedimiento administrativo disciplinario para los/as usuarios/as que presuntamente hayan incumplido con las políticas de seguridad de la información de la BNP, a fin de realizar las acciones conforme al marco normativo vigente.

- Los siguientes lineamientos podrían ser considerados en el procedimiento administrativo disciplinario:
  - Verificar previamente que el incumplimiento a la seguridad de la información haya ocurrido.

- Asegurar el debido procedimiento, así como, un correcto y justo tratamiento de los/as usuarios/as que presuntamente hayan incumplido con la seguridad de la información.

g. **Término del vínculo laboral, ausencia temporal o cambio de funciones o de puesto**

- En los supuestos de término del vínculo laboral, ausencia temporal o cambio de funciones o de puesto, la Oficina de Administración a través del Equipo de Trabajo de Recursos Humanos, en coordinación con el/la Oficial de Seguridad de la Información, deberá comunicar al/a la usuario/a, aspectos relacionados a la seguridad de la información, tales como, las responsabilidades y tareas que subsistirían.

- Cuando se produzca ausencia temporal y/o vacaciones del/de la usuario/a, el órgano al cual pertenece deberá notificar a la Oficina de Tecnologías de la Información y Estadística la necesidad de bloquear provisionalmente los accesos a cargo del/de la usuario/a durante la vigencia de su ausencia.

h. **Retorno de activos de información**

- El término del vínculo laboral, contrato u orden de servicio debe incluir el retorno previo del software, documentación, equipos, dispositivos móviles, llaves, tarjetas de identificación, información guardada en medios electrónicos, entre otros activos de información de la BNP, según lo definido en las Políticas para la Seguridad Física y Ambiental.

i. **Retiro de los derechos de acceso**

- El término del vínculo laboral debe incluir el retiro de los derechos de acceso a la información, servicios de tratamiento de información y a las instalaciones de procesamiento de información, es decir, retiro de accesos lógicos y físicos, según lo definido en las Políticas para el Control de Acceso.

- En caso de cambio de funciones o de puesto, los derechos de acceso a la información, servicios de tratamiento de información y a las instalaciones de procesamiento de información deben ser revisados y de ser necesario modificados y/o retirados los que no fueron aprobados para las nuevas funciones o puesto.

- Los derechos de acceso para activos de información, servicios de tratamiento de información e instalaciones de procesamiento de información deben ser revocados al término del vínculo laboral, o cambio de funciones o de puesto, dependiendo de la evaluación de los factores de riesgo.

6.2. Políticas para la gestión de activos de información

6.2.1. Objetivos

- Mantener una protección adecuada sobre los activos de información de la BNP.
- Asegurar la clasificación de activos de información, según lo definido por la BNP.

6.2.2. Alcance

Estas políticas deben ser cumplidas por los/as usuarios/as de los distintos órganos de la BNP.

La gestión de la seguridad de la información comprende todos los activos de información que la BNP posee en la actualidad y a futuro. Las políticas cubren toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo electrónico o usada en medios electrónicos o en forma verbal.

6.2.3. Políticas

a. Responsabilidades sobre los de activos de información

- Los activos de información de la BNP deben ser claramente identificados y registrados en un inventario de activos de información, el cual debe ser actualizado anualmente, para ello se cuenta con el Procedimiento de Inventario, Etiquetado y Tratamiento de Activos de Información.
- Todos los activos de información deben tener un "Propietario" quien debe ser responsable de asegurar la apropiada clasificación y protección de los mismos; para lo cual, debe definir y revisar periódicamente las restricciones de acceso y las clasificaciones.
- Se debe cumplir con todos los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo los lineamientos de seguridad de la información que deben mantenerse alineados con las leyes vigentes.
- Todo aquel que ponga en riesgo los activos de información de la BNP debe ser sancionado, conforme al marco normativo vigente.
- Se debe reportar a un nivel apropiado y lo antes posible, cualquier incidente que ponga en riesgo los activos de información para que se tomen las medidas necesarias.

b. Clasificación de la información

- Los criterios que deben ser aplicados para clasificar la información son las siguientes:

Tabla 01 - Clasificación de la Información

Clasificación de Información	Definición
Confidencial	Activos de información cuyo contenido no debe ser divulgado ni distribuido a personas que no sean autorizadas y cuya difusión genere un impacto importante en la entidad entre ellas: pérdida económica, sanción legal o pérdida de imagen institucional.
Uso Interno	Activos de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno de la entidad.
Público	Información no sensible de acceso público y que su divulgación no genere impacto en la entidad.

- No se debe divulgar información de la BNP, que haya sido clasificada como "Confidencial" o de "Uso Interno", salvo que haya sido expresamente autorizado por el Propietario de Información quien será responsable de dicha divulgación.

- Se debe solicitar autorización por escrito y/o correo electrónico al Propietario de Información, cuando se necesite proporcionar información "Confidencial" o de "Uso Interno" a terceros. La entrega de esta información se debe realizar suscribiendo declaraciones de confidencialidad y no divulgación con el tercero y/o aplicando los controles específicos que se definan.

- Toda información no clasificada será considerada de "Uso Interno", de manera que reciba los niveles de protección en base a esta clasificación.

- Se deben rotular los activos de información según su clasificación, esto incluye a la información impresa y digital, según el Procedimiento de Inventario, Etiquetado y Tratamiento de Activos de Información.

c. **Manejo de los medios de almacenamiento**

- La Oficina de Tecnologías de la Información y Estadística debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario/a.

- La información física y digital de la BNP debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales. Este período debe ser indicado en las tablas de retención documental que gestiona la BNP; y, cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

- Los/as usuarios/as deben tener en cuenta estas consideraciones cuando impriman, escaneen y saquen copias: verificar las áreas adyacentes a impresoras, escáneres y equipos de fotocopiado para asegurarse que no quedaron documentos relacionados o adicionales. Así también, recoger de las impresoras, escáneres y equipo de fotocopiado, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

- Los/as usuarios/as deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores. Estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

- Los órganos de la BNP deben utilizar los medios para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma (ejemplo: máquinas trituradoras, etc.).

- La Oficina de Tecnologías de la Información y Estadística debe gestionar el contrato de almacenamiento y resguardo de las cintas de backup, otros medios de almacenamiento y documentos físicos de la BNP con el proveedor del servicio. Así también, debe verificar el cumplimiento de los Acuerdos de Niveles de Servicio y Acuerdos de intercambio con el proveedor de custodia externo de los medios de almacenamiento y documentos de la entidad.

6.3. Políticas para el control de acceso

6.3.1. Objetivos

- Controlar el acceso a la información confidencial y servicios de tratamiento de información de la BNP, para proteger la integridad, confidencialidad y disponibilidad de la información.
- Asegurar el acceso autorizado de usuarios/as y prevenir accesos no autorizados a los sistemas de información.
- Evitar el acceso de usuarios/as no autorizados, evitar poner en peligro la información y evitar el robo de información y los servicios de tratamiento de información.
- Evitar el acceso no autorizado a los servicios de la red y sistemas de información.

6.3.2. Alcance

Estas políticas deben ser cumplidas por los/as usuarios/as de los distintos órganos de la BNP.

6.3.3. Políticas

a. **Gestión de acceso de los/as usuarios/as**

- Con el propósito de impedir accesos no autorizados a los activos de información, deben establecerse procedimientos formales para asignar los derechos de acceso a los mismos.
- Los responsables de los distintos órganos serán los encargados de autorizar y solicitar el acceso de los/as usuarios/as a su cargo, a los recursos de tecnologías de información según esta política. Asimismo, deben informar y solicitar a la Oficina de Tecnologías de la Información y Estadística la cancelación de accesos en caso que un/a usuario/a deje de pertenecer a la BNP o cuando sus funciones ya no lo requieran.
- La Oficina de Tecnologías de la Información y Estadística debe asignar un identificador (cuenta) único y exclusivo a toda persona que haga uso de los activos de información ya sea de forma temporal o permanente y que le permita contar con el mínimo acceso autorizado para el normal desarrollo de sus actividades.
- Se debe controlar que no se compartan identificadores entre diferentes usuarios/as. Para ello, deben definirse lineamientos de control a nivel sistema operativo y/o de red, de manera que se pueda detectar duplicidad de sesiones de usuarios/as.
- La Oficina de Tecnologías de la Información y Estadística debe establecer los lineamientos en la red informática para permitir que el/la usuario/a pueda cambiar su contraseña en caso de que lo requiera (incluyendo el primer inicio de sesión).

b. **Responsabilidad de los/as usuarios/as**

- Los/as usuarios/as son responsables de la confidencialidad de la contraseña asignada; y, de las consecuencias por las acciones que terceras personas puedan hacer con el uso de la misma.
- El/La usuario/a debe cambiar su contraseña regularmente o cada vez que el sistema se lo solicite. No está permitido compartir las contraseñas asignadas.
- Para realizar la restauración de contraseñas se debe seguir un procedimiento formal de comunicación establecido por la Oficina de Tecnologías de la Información y Estadística para la restauración de contraseñas por pérdida u olvido de la anterior.
- El/La usuario/a debe bloquear su estación de trabajo si por algún motivo se retira de su puesto de trabajo.
- Todas las estaciones de trabajo deben tener un protector de pantalla con clave y activación automática de bloqueo de usuario cuando no se estén utilizando.
- El/La usuario/a debe mantener sus escritorios libres de documentos y/o medios de almacenamiento removibles cuando no los utilice, procurando guardarlos en gabinetes con llaves.

c. **Control de acceso al sistema operativo**

- El acceso al sistema operativo de las estaciones de trabajo de la BNP debe tener controles de seguridad (por ejemplo, usuario y contraseña), a fin de evitar accesos no autorizados a recursos o información.
- Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen los siguientes:
  - Identificación automática de estación de trabajo.
  - Procedimiento de inicio de sesión seguro.
  - Identificación y autenticación de usuarios.
  - Sistema de gestión de contraseñas.
  - Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad.
  - Desconexión automática de computadoras por tiempo de inactividad.
  - Limitación de acceso por horarios de trabajo y tiempo de conexión.

d. **Control de acceso a los sistemas de información**

- Se deben establecer los lineamientos de control de accesos a la información y a los sistemas de información, restringiendo el acceso únicamente para el/la usuario/a debidamente autorizado.
- Los accesos concedidos deben revisarse periódicamente, revocando los derechos del/de la usuario/a cuya vigencia de autorización haya caducado.
- Se deben aislar los sistemas identificados con información sensible asignándoles un entorno de procesamiento dedicado, creado a partir de métodos físicos o lógicos (por ejemplo, contraseñas o control de acceso biométrico).

e. **Control de acceso físico**

- Los/as usuarios/as de la BNP, terceros autorizados o visitantes, deben portar siempre su identificación en un lugar visible al permanecer en las instalaciones de la BNP.

- Los visitantes autorizados para ingresar a las instalaciones de la BNP deben portar en forma permanente y en un lugar visible su identificación como visitantes, firmar el registro de ingreso cuando entren a las instalaciones de procesamiento de datos o áreas de acceso restringido por los responsables de los órganos de la entidad.

- El acceso de visitantes al centro de datos, los repositorios, la bóveda o áreas de trabajo que contengan información sensible debe estar físicamente restringido y el ingreso de visitantes se debe realizar con el acompañamiento de un/a usuario/a de la BNP debidamente autorizado.

- Se deben mantener registros del ingreso a las áreas identificadas como de acceso restringido, indicando el nombre de la persona que ingresa, documento de identificación, fecha, hora de entrada y salida, y motivo de la visita.

- La Oficina de Tecnologías de la Información y Estadística debe clasificar como de acceso restringido, los lugares donde se encuentren equipos de comunicaciones (*switches, routers, firewalls* y consolas de administración, etc.).

- Todos los órganos de la BNP adoptarán medidas de seguridad definidas en el sistema de gestión de seguridad de la información que permitan proteger las áreas con acceso restringido como los repositorios, la bóveda, el centro de datos o cuartos de equipos con controles de seguridad apropiados en donde incluyan lo siguiente: detección de incendios, control de humedad, protección contra ingreso, alarmas, sistemas de extinción de incendios y videocámaras de acuerdo con los riesgos de seguridad de la información identificados para cada área.

- No se debe permitir el uso de equipos como cámaras fotográficas, grabadoras de vídeo o audio en áreas restringidas de la BNP sin contar antes con la autorización formal del responsable del órgano.

- El traslado de equipos de cómputo, comunicaciones, dispositivos móviles de la BNP debe ser autorizado por el responsable del órgano al cual pertenece el equipo. Ésta autorización debe contener como mínimo, el nombre e identificación de la persona responsable del activo, la identificación del equipo que se traslada, origen y destino, además, la fecha del traslado.

- La Oficina de Tecnologías de la Información y Estadística debe contar con la lista de usuarios/as autorizados/as para ingresar a su centro de datos y áreas restringidas de procesamiento de datos de la entidad.

f. **Control de acceso a la información**

- Los/as usuarios/as y prestadores/as de servicios deben aplicar todos los controles de seguridad definidos por la entidad para garantizar la preservación de la Confidencialidad, Integridad y Disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades o bien por otras situaciones esté bajo su custodia.

- Los/as usuarios/as y prestadores/as de servicios que realicen actividades para la BNP deben tener acceso únicamente a la información necesaria para el desempeño de las actividades que le han sido autorizadas.

- Todo acceso a la información debe ser autorizado formalmente por el órgano responsable de la información. Para la autorización de acceso a la información se debe contemplar un análisis previo de la justificación de la necesidad de uso de la misma y las actividades a realizar con el acceso a la información.

- Todo acceso a la información debe considerar el nivel de clasificación definido por la BNP o por el responsable de la información.

- Todo acceso a la información debe cumplir con los requisitos legales, normativos, reglamentarios, procedimentales o de cualquier otra índole que haya definido el responsable de la información.

- El acceso a la información de la BNP debe estar sujeto a controles que garanticen la trazabilidad de las acciones realizadas sobre la misma, considerando la identificación del/de la usuario/a o prestador/a de servicios que realice el acceso, acciones realizadas, instante de tiempo en que se realizan las acciones y ubicación desde la cual se realiza el acceso a la misma.

- Se consideran usos no autorizados de la información, lo siguiente:
  - Modificar la información sin contar con la autorización formal para ello.
  - Modificar o eliminar los controles de seguridad que protejan la información.
  - Impedir el acceso a la información sin justificación real.
  - Divulgación no autorizada de información.

6.4. Políticas para la seguridad física y ambiental

6.4.1. Objetivos

- Establecer mecanismos de seguridad física y ambiental a fin de evitar el acceso de usuarios/as no autorizados/as, daños e interferencias contra las instalaciones y la información de la BNP.

- Evitar la posibilidad de pérdidas, daños y/o comprometer la infraestructura de la BNP por causas ambientales, vandalismo, robo y otro que pueda interrumpir las operaciones.

6.4.2. Alcance

Estas políticas deben ser cumplidas por los/as usuarios/as de los distintos órganos de la BNP; y, por los/as prestadores/as de servicios

La gestión de la seguridad física está a cargo del Equipo de Trabajo de Operaciones y Mantenimiento de la Oficina de Administración, a través del servicio de seguridad y vigilancia, y es responsabilidad de los/as usuarios/as y prestadores/as de servicios el cumplimiento de los lineamientos dispuestos.

6.4.3. Políticas

a. **Perímetro de seguridad física**

- El perímetro de seguridad física debe estar claramente definido y demarcado.

- Se deben proteger las áreas donde funcionan las instalaciones de procesamiento de información, suministro de energía eléctrica, aire acondicionado y cualquier otra que sea considerada como crítica y que pudiera afectar el funcionamiento de los sistemas de información.

b. **Controles físicos de entradas**

- En los accesos a la entidad se deberá contar con controles que aseguren el acceso físico sólo a usuarios/as debidamente autorizados/as. En caso de prestadores/as de servicios se deberá contar con autorización expresa del responsable del órgano que gestionará las actividades así como las responsabilidades de estos.

- El acceso y la permanencia de visitas sólo serán permitidos para propósitos específicos y con autorización respectiva, quedando debidamente registrados. En el registro se debe considerar como mínimo la siguiente información: el nombre de la persona que autoriza el ingreso, la hora y fecha de entrada y salida de la visita, el motivo de la visita, el órgano en el cual permanecerá la visita durante su estancia.

c. **Seguridad en oficinas e instalaciones de la BNP**

- Se deben diseñar y aplicar los controles de seguridad física en las oficinas e instalaciones de la BNP dedicadas al procesamiento de la información.

- Aquellas áreas dedicadas al procesamiento de información deben ser ubicadas en un lugar que no presenten riesgos desde el punto de vista de acceso al público.

- No deben ponerse a libre disposición del público guías ni listados que brinden información de ubicaciones y cualquier otro dato relacionado con las instalaciones críticas de procesamiento de la información.

- Se debe controlar el ingreso de computadoras portátiles, equipos fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, mediante autorización expresa del responsable del órgano visitante y de la Oficina de Tecnologías de la Información y Estadística.

- Se debe prohibir comer, beber dentro de las áreas de trabajo.

d. **Trabajo en las áreas seguras**

- Todas las áreas seguras deben tener acceso restringido y ser monitoreadas por el personal de vigilancia en todo momento.

- Se debe llevar un registro (físico o digital) del ingreso a las áreas seguras, el cual contendrá como mínimo los siguientes campos: fecha, hora de entrada y salida, motivo de la visita, nombre de la persona que autoriza su ingreso, nombre de la persona que está ingresando.

e. **Acceso a áreas de carga y descarga**

Los accesos al área de carga y descarga serán restringidos únicamente a usuarios/as autorizados/as y que estén debidamente identificados/as.

f. **Seguridad de activos de información**

Con el propósito de evitar daños o pérdidas derivados de la indisponibilidad de la continuidad de los procesos que se realizan en la BNP, es necesario implementar controles para la debida protección de los activos de información.

g. **Protección de infraestructura segura**

- Se debe diseñar y aplicar protección física contra daños por fuego, inundación, terremoto y otras formas de desastre natural o generados por el hombre.
- Todo material inflamable debe almacenarse en lugares que no puedan comprometer las áreas seguras.
- Los repositorios, la bóveda, el centro de datos de la BNP, deben contar con un sistema automático de protección contra incendios, teniendo un control de fácil acceso.

  Se debe implementar un sistema de monitoreo automático y/o manual de las condiciones ambientales de temperatura y humedad para que no afecten el normal funcionamiento de los equipos de tratamiento de información. Este sistema debe tener un control de fácil acceso.

h. **Suministro de energía eléctrica**

Se deben proteger los equipos informáticos de fallas por suministro de energía y otras anomalías eléctricas. La provisión de energía debe ser provista conforme a las especificaciones del fabricante de equipos. Asimismo, se debe considerar el incluir equipos de energía ininterrumpida (UPS) para los equipos que soportan las operaciones críticas de la BNP y, de ser posible, contar con un generador de energía (grupo electrógeno) en casos de interrupciones prolongadas de suministro de energía eléctrica.

i. **Protección del cableado**

- El cableado de las redes de datos y de comunicaciones, y suministro de energía eléctrica debe protegerse para evitar una interceptación o daño.
- El cableado de la red de datos debe cumplir con los estándares internacionales de cableado estructurado; cada elemento debe estar identificado, etiquetado y debe mantenerse una memoria técnica descriptiva actualizada.
- El cableado de suministro de energía eléctrica y telecomunicaciones en las zonas de tratamiento de información, debe contar con un sistema de puesta a tierra (pozo a tierra), el que debe ser revisado periódicamente para garantizar su adecuado funcionamiento.

j. **Mantenimiento de equipos**

Se debe considerar un programa de mantenimiento preventivo y correctivo de los equipos de soporte a los procesos de la entidad, sistemas de acondicionamiento de temperatura, humedad y filtrado de aire, sistemas de energía ininterrumpida y sistemas de detección y extinción de fuego según las especificaciones del fabricante.

BIBLIOTECA NACIONAL DEL PERÚ V°B° Eduardo Roncal OTIE

BIBLIOTECA NACIONAL DEL PERÚ V°B° Augusto Fernandini OPP

BIBLIOTECA NACIONAL DEL PERÚ V°B° Eduardo Ulloa OPP EMO

BIBLIOTECA NACIONAL DEL PERÚ V°B° Gerald Benavente Q. Jefe E.T. Log. y C.P. Oficina de Administración

BIBLIOTECA NACIONAL DEL PERÚ Oficial de Seguridad de la Información

k. **Seguridad de equipos fuera del local**

El uso de equipos de la entidad fuera del local debe ser autorizado, y el/la usuario/a autorizado/a será responsable de su custodia. La autorización del uso fuera de las instalaciones de la entidad deberá ser coordinada con el Equipo de Trabajo de Logística y Control Patrimonial de la Oficina de Administración.

l. **Eliminación segura o reutilización de equipos**

La Oficina de Tecnologías de la Información y Estadística debe asegurar que la información sensible contenida en los equipos haya sido eliminada o sobrescrita de manera segura antes de ser reutilizados o desechados de modo que su recuperación sea irreversible.

m. **Retirada de materiales de propiedad de la BNP**

Se debe contar con autorización formal para el retiro de materiales como equipos, información o software que son de propiedad de la BNP.

6.5. Políticas para la seguridad de las operaciones

6.5.1. Objetivos

- Asegurar la operación correcta y segura de los servicios de tratamiento de información.
- Implementar y mantener un nivel apropiado de seguridad de la información y entrega de servicio.
- Verificar la implementación de acuerdos, el monitoreo de la conformidad con los acuerdos y los cambios gestionados con el fin de asegurar que todos los servicios entregados cumplan con todos los requerimientos acordados.
- Proteger la confidencialidad e integridad del software y de la información. Establecer pautas y precauciones para prevenir y detectar software malicioso.
- Establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo, haciendo copias de seguridad y realizando pruebas para su oportuna recuperación.
- Establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, entre los principales), datos de entrada o salida y documentación del sistema, de daño, modificación, robo y acceso no autorizado.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para el monitoreo del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

6.5.2. Alcance

Estas políticas deben ser cumplidas por la Oficina de Tecnologías de la Información y Estadística de la BNP.

6.5.3. **Políticas**

a. **Responsabilidades de operación**

- La Oficina de Tecnologías de la Información y Estadística deberá asegurar la existencia de documentación formal de sus procedimientos operativos, estableciendo las responsabilidades y los recursos utilizados para su ejecución eficiente.

- La Oficina de Tecnologías de la Información y Estadística debe asegurar que todos los equipos de la infraestructura tecnológica deben estar instalados en ubicaciones físicas que cuenten con las medidas de seguridad mínimas para evitar, pérdida, robo, actos vandálicos; y, en general, protegidos de amenazas, peligros del entorno y accesos no autorizados.

- La Oficina de Tecnologías de la Información y Estadística deberá asegurar que cada operador tenga una cuenta de acceso única, personal e intransferible para el uso de equipos informáticos ubicados en el Centro de Datos.

b. **Separación de los ambientes para desarrollo, pruebas y producción**

- Se deben separar los ambientes de desarrollo, prueba y producción implementando los controles necesarios, asimismo, se debe definir y documentar el procedimiento para implementaciones en producción.

- El ambiente de pruebas debe ser lo más parecido al ambiente de producción.

- En caso de utilizar información real en el ambiente de pruebas, ésta se debe enmascarar utilizando algún software.

c. **Planificación y aceptación del sistema**

- La Oficina de Tecnologías de la Información y Estadística debe supervisar la planificación de capacidades de los aplicativos en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado.

- La Oficina de Tecnologías de la Información y Estadística debe establecer los criterios y las pruebas a realizar a los aplicativos existentes o nuevos, que permitan al área usuaria su evaluación y aceptación formal previo a su implementación en los ambientes de producción.

d. **Gestión de cambios**

- La Oficina de Tecnologías de la Información y Estadística deberá mantener un registro de control de cambios de los sistemas de información, equipos de comunicaciones, bases de datos, equipos de cómputo y perfiles de acceso a través de la implementación de acciones y procedimientos necesarios para asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de comprobación y estrés, controles de seguridad, reversión en caso de fallas y análisis de impacto.

- Todos los cambios deben ser solicitados a la Oficina de Tecnologías de la Información y Estadística por el propietario de la información, y se llevará un registro sobre cada solicitud de cambio. En caso existiera algún problema con el

cambio realizado se revertirá al estado anterior al cambio, según lo especificado en el procedimiento de gestión de cambios.

- Todas las solicitudes de controles de cambio serán evaluadas para validar si el cambio afecta tanto al componente como al contexto donde se encuentra.
- Los cambios que se realicen a la infraestructura de tecnologías de la información de la entidad se debe verificar la necesidad de actualizar los planes de contingencia y continuidad de negocio.
- Se deben documentar los cambios hechos por la BNP en cuanto a mejoras de los servicios actuales ofrecidos por terceros, desarrollo de todos los sistemas de información nuevos, controles nuevos para resolver los incidentes de seguridad de la información, modificaciones o actualizaciones de los lineamientos y procedimientos de la entidad, teniendo en cuenta la importancia de los sistemas y procesos involucrados.
- Se deben gestionar los servicios a implementar por terceros como: cambios y mejoras en las redes, uso de nuevas tecnologías, actualización de productos nuevos o nuevas versiones, nuevas herramientas y entornos de desarrollo, cambios de la ubicación física de las instalaciones de los servicios y cambio de proveedores.
- No se deben aceptar cambios por parte de la prestación del servicio de terceros, sin el previo estudio, aprobación y su debida documentación.
- No se debe poner en peligro la integridad de la información debido a la falta de revisión de los cambios.
- No se pueden realizar cambios que atenten o vayan en contra de las estrategias de continuidad y seguridad definidas por la BNP.

e. **Gestión de vulnerabilidades técnicas**

- El/La Oficial de Seguridad de la Información debe programar la realización de pruebas de comprobación técnica a cargo de especialistas externos para verificar que se han implementado correctamente los controles de seguridad definidos para el hardware y software.
- Identificadas las vulnerabilidades técnicas, se deben determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Los sistemas críticos y en alto riesgo deben ser tratados primero.
- Para la aplicación de una actualización de seguridad (parches) se debe probar y evaluar su efectividad en un ambiente de pruebas, asimismo, se deben conocer y considerar los riesgos asociados a su aplicación y en todos los casos se debe cumplir con los controles establecidos para la gestión de cambios según el procedimiento de gestión de cambios.
- Es necesario que la Oficina de Tecnologías de la Información y Estadística, responsable de la plataforma tecnológica tenga un inventario actualizado de los activos de información.
- Se debe identificar la necesidad de iniciar un análisis de vulnerabilidades cuando:

- Se realiza una solicitud de la Alta Dirección o de los custodios de los activos de información tecnológicos.
- Se realiza un cambio significativo en un componente de la infraestructura tecnológica.
- Se realiza por cumplimiento regulatorio.
- Se apruebe el plan para el escaneo de vulnerabilidades.
- Se determine los componentes que serán objeto de gestión de vulnerabilidades.
- Se determine las acciones necesarias ante posibles incidentes durante la ejecución de escaneos.
- Se revise y garantice el buen funcionamiento de la herramienta de escaneo
- Se analice, consolide recomiende y se genere informes de las vulnerabilidades detectadas.
- Se realiza seguimiento a los planes de remediación y medidas de control correspondientes de las vulnerabilidades reportadas.

f. **Protección contra software malicioso y móvil**

- La Oficina de Tecnologías de la Información y Estadística deberá de adoptar las medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de servidores de red, computadores portátiles, estaciones de trabajo y dispositivos móviles.
- La Oficina de Tecnologías de la Información y Estadística debe asegurar que todas las estaciones de trabajo estén protegidas con el antivirus corporativo, el cual debe estar actualizado. Asimismo, el sistema operativo y los aplicativos de oficina deben contar con las últimas actualizaciones de seguridad (parches).
- La Oficina de Tecnologías de la Información y Estadística es responsable de la renovación de licencias de software, y deberá de definir su cronograma de renovación, para evitar que se produzca incumplimiento de uso legal de software.
- El software utilizado por la BNP debe ser autorizado en forma expresa por el responsable de la Oficina de Tecnologías de la Información y Estadística.
- El usuario final no debe tener el privilegio de deshabilitar los sistemas de control y prevención de malware.
- La Oficina de Tecnologías de la Información y Estadística, como medida de prevención, al detectar que algún servidor de red, estación de trabajo o computadora portátil está infectada con algún tipo de malware deberá ejecutar el proceso de desinfección respectivo. En caso no se pueda desinfectar el equipo, se procederá a aislarlo de la red de la BNP inmediatamente.

g. **Gestión de respaldo y recuperación**

- La Oficina de Tecnologías de la Información y Estadística deberá establecer procedimientos rutinarios para el respaldo de la información de acuerdo a la clasificación de la misma, realizando copias de seguridad y pruebas de recuperación conforme a un cronograma definido y según lo especificado en el procedimiento de respaldo y recuperación de la información.
- Las copias de seguridad deben resguardarse en un lugar externo al de la entidad que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad. Asimismo, los equipos y los medios de respaldo deben estar a una

distancia determinada para evitar que se dañen por un desastre en el Centro de Datos.

- Los equipos y los medios de respaldo deben contar con un programa de mantenimiento preventivo y correctivo para asegurar su correcto funcionamiento.
- La Oficina de Tecnologías de la Información y Estadística debe estimar anticipadamente la cantidad necesaria de medios magnéticos requeridos para realizar las copias de respaldo y en caso de no contar con ello solicitar su oportuna adquisición al área correspondiente.
- Las copias de respaldo se deben programar y realizar pruebas periódicamente para verificar que cumplen con los propósitos para las cuales fueron realizadas. Los resultados serán utilizados para actualizar los procedimientos de respaldo, recursos tecnológicos necesarios, evidenciar oportunidades de mejora o riesgos en la realización de copias de respaldo y restauración de información.
- Los responsables de los órganos de la BNP deben informar a la Oficina de Tecnologías de la Información y Estadística, qué datos son los necesarios para el cumplimiento de sus funciones para poder establecer las copias de respaldo.

h. **Uso adecuado de los recursos y servicios informáticos**

- Los recursos y servicios informáticos asignados a los/as usuarios/as de la BNP son de uso exclusivo para las funciones encomendadas a su cargo. Está prohibido utilizarlos para cualquier otra actividad que no forme parte de sus labores.
- Los/as usuarios/as que hagan uso de los servicios y recursos de tecnología de información de la BNP, deben cumplir, según corresponda, con las normas establecidas en los reglamentos, directivas, procedimientos e instructivos aprobados.
- Los/as usuarios/as que incumplan con lo establecido en las normas quedarán sujetos/as a las sanciones establecidas en el marco normativo vigente,

i. **Registros de auditoría y monitoreo**

- Deben generarse registros de auditoría sobre el uso de los recursos de tecnología de información.
- Las actividades de operadores y administradores de los sistemas deben ser monitoreadas, registradas y verificadas regularmente por el/la Oficial de Seguridad de la Información.
- Se debe contar con registro de fallas en los sistemas para asegurar que han sido corregidas oportunamente.
- Se debe generar respaldo de la información de los registros de auditoría y monitoreo.
- Los/as usuarios/as de la BNP son responsables de todas las actividades realizadas con sus cuentas de acceso a red, correo electrónico y sistemas de información asociados a la entidad.

6.6. Políticas para la seguridad de las comunicaciones

6.6.1. Objetivos

- Mantener la confidencialidad, integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.
- Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones, normando la realización de acuerdos formales para el intercambio de software o de información, de acuerdo a la legislación correspondiente.
- Detectar las actividades de procesamiento de información no autorizadas, estableciendo el monitoreo de los sistemas, así como, la grabación de los eventos de seguridad de información, como el registro de operadores y de las fallas para asegurar que los problemas del sistema de información sean identificados, dentro de los límites de la legislación vigente.

6.6.2. Alcance

Estas políticas deben ser cumplidas por la Oficina de Tecnologías de la Información y Estadística de la BNP.

6.6.3. Políticas

a. **Segregación de tareas**

- Se deben generar perfiles de trabajo de acuerdo a las necesidades de cada proceso y en concordancia con el objetivo de la entidad. Cada usuario/a deberá tener asignado un perfil, con el cual tendrá tareas, actividades y permisos predefinidos.

b. **Gestión y niveles de servicios externos**

- Se debe asegurar que todos los controles de seguridad y los acuerdos de niveles de servicio (SLA) sean implementados y cumplidos.
- Los servicios brindados por los/as prestadores/as de servicios deben ser monitoreados, gestionados y auditados regularmente.
- Los cambios en los servicios brindados por los/as prestadores/as de servicios deben ser planificados y autorizados considerando los riesgos que podrían generar.
- Los/as y prestadores/as de servicio que cuenten con acceso a información interna de la BNP deberán tener asignado una cuenta de usuario con acceso únicamente a la información necesaria.

c. **Diseño de la infraestructura de seguridad en la red informática**

- La Oficina de Tecnologías de la Información y Estadística debe implantar los controles y medidas requeridas para proteger y conservar la seguridad de los datos en la red interna la BNP y la protección de los servicios, que requieran conectividad, contra accesos no autorizados. Estos controles deben incluir lo siguiente:
  - Implementar un esquema de segmentación de la red interna de la BNP.

- Monitoreo (manual o automático) de la red interna de la BNP y los activos de información conectados a la misma.
- Coordinación de las actividades de gestión para optimizar el servicio de la red interna de la BNP y asegurar que los controles se apliquen adecuadamente a través de toda la infraestructura de procesamiento de la información.
- Se deben establecer controles y medidas especiales para salvaguardar la confidencialidad y la integridad de los datos que pasen a través de redes públicas, así como, para proteger los aplicativos conectados utilizando hardware tales como firewall, UTM (gestión unificadas de amenazas), IPS/IDS, filtro de contenidos, anti spam, entre otros.

d. **Buen uso de los medios de almacenamiento**

- Con la finalidad de prevenir interrupciones a los procesos de la BNP y asegurar el procesamiento de información que hace posible que estos procesos se realicen, se deberá contar con mecanismos de seguridad que garanticen que los medios de almacenamiento donde se resguarda la información de los procesos sean controlados y protegidos físicamente.

- Asimismo, la Oficina de Tecnologías de la Información y Estadística debe implementar los controles que aseguren que todos los medios de almacenamiento que contienen información sensible sean almacenados, protegidos contra el acceso no autorizado y eliminados de manera segura y efectiva.

e. **Acuerdos de intercambio de información**

- Se utilizarán declaraciones de confidencialidad y no divulgación con los/as usuarios/as y prestadores de servicios, si por su trabajo u otras razones requieran conocer o intercambiar información sensible o de uso interno de la BNP. En estos acuerdos se especificarán de forma explícita las responsabilidades para el intercambio de la información para cada una de las partes; y, se deberán firmar antes de permitir el acceso o uso de dicha información.

6.7. Políticas para el desarrollo y mantenimiento de sistemas de información

6.7.1. Objetivos

- Prevenir error, pérdida, modificación no autorizada o mal uso de la información en los sistemas de información.
- Garantizar la seguridad de los archivos de configuración de las aplicaciones.
- Mantener la seguridad de la información y el software en los sistemas de información de la BNP.
- Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas de los sistemas de información de la BNP.

6.7.2. Alcance

Estas políticas deben ser cumplidas por la Oficina de Tecnologías de la Información y Estadística de la BNP.

Los procedimientos y técnicas orientados a mitigar los riesgos de seguridad de la información en el desarrollo y mantenimiento de sistemas de información deben ser aplicados en todas las plataformas, ambientes y desarrollos internos o tercerizados.

6.7.3. **Políticas**

a. **Metodología para el desarrollo y mantenimiento de sistemas de información**

- La BNP debe tener una metodología estandarizada para el desarrollo y mantenimiento de sistemas de información.
- Todo desarrollo y/o mantenimiento de sistemas de información será documentado, a fin de garantizar la continuidad del uso de los sistemas de información implementados en la BNP, y que se ejecuten las actividades con facilidad.

b. **Requisitos de seguridad de la información**

- Se debe definir un procedimiento de control y nivel de seguridad de la información, en el proceso de desarrollo de todo sistema de información.
- Todo sistema de información desarrollado por la Oficina de Tecnologías de la Información y Estadística así como por prestadores/as de servicios, debe satisfacer los requisitos de seguridad de la información definidos para el desarrollo y mantenimiento de los sistemas. En caso que los sistemas de información sean desarrollados por prestadores/as de servicios, los requisitos de seguridad de la información deben ser mencionados en los términos de referencia.
- La Oficina de Tecnologías de la Información y Estadística y los terceros deben cumplir con los controles y metodologías establecidos por la BNP, los cuales podrán ser revisados.
- La Oficina de Tecnologías de la Información y Estadística debe verificar que los acuerdos suscritos con los prestadores/as de servicios, incluyan cláusulas referidas a la cesión de derechos de información y de confidencialidad con el personal involucrado para el resguardo de la propiedad intelectual de la BNP y de la confidencialidad de la información.
- Todo sistema de información desarrollado por la Oficina de Tecnologías de la Información y Estadística o terceros es propiedad de la BNP.
- Los responsables de los órganos deben definir los lineamientos a considerar en el desarrollo y/o mantenimiento de sistemas de información, a fin de definir los controles respectivos para la validación, seguimiento de la integridad de los datos almacenados, y el registro de actividades en el sistema de información.

c. **Procesamiento correcto de los sistemas de información**

- Se deben realizar comprobaciones periódicas y/o aleatorias de la información que generan los aplicativos y/o sistemas de información para validar los datos de salida. Asimismo, deben definirse las responsabilidades de todos los implicados en el proceso de salida de datos.
- Deben identificarse los requerimientos para asegurar la autenticidad y la integridad de los mensajes en los sistemas de información, debiendo definirse e implementarse los controles apropiados.

d. **Seguridad de los datos del sistema de información**

- Se deben implementar controles sobre lo siguiente:
  - Protección de datos del sistema de información: Implementar un procedimiento para enmascarar los datos sensibles, en ambientes de prueba.

e. **Control de acceso al código fuente del sistema de información**

- Se debe restringir y controlar el acceso al código fuente de los sistemas de información únicamente al personal autorizado para su edición y/o modificación.
- Se debe contar con un responsable del acceso al código fuente de los sistemas de información, quien deberá implementar un registro de uso si es que el código es requerido.
- Se debe implementar un proceso automático y/o manual que permita controlar las versiones del código fuente.

f. **Seguridad en los procesos de desarrollo y pase a producción**

- Análisis de requerimientos del sistema de información
  - Se deben definir los requerimientos referidos a arquitectura, tecnología necesaria, seguridad de la información y otros requerimientos especiales.
- Procedimiento para el desarrollo del sistema de información
  - Se debe utilizar una metodología de desarrollo de sistemas de información (propia o estándar).
  - La metodología de desarrollo de sistemas de información de la BNP debe considerar, como mínimo, las siguientes etapas:
    - ❖ Especificación de requerimientos (funcionales y no funcionales).
    - ❖ Análisis y diseño (especificación detallada del sistema de información y definición de la arquitectura del sistema de información).
    - ❖ Desarrollo del sistema (construcción del sistema de información).
    - ❖ Pruebas de calidad de software.
    - ❖ Implementación y entrenamiento (entrega del sistema, aprobación del sistema y entrenamiento).
    - ❖ Pase a producción (implementación del sistema de información).
    - ❖ Manuales de usuario/a y de administrador/a (realizar el manual de uso y el manual técnico).
- Pase a producción
  - El Equipo de Trabajo de Desarrollo de Sistemas de Información de la Oficina de Tecnologías de la Información y Estadística y terceros, encargados del desarrollo y mantenimiento de los sistemas de información, no tendrán acceso a los datos de producción.
  - Los ambientes de desarrollo y producción deben ser configurados, a fin de limitar el acceso a estos solo al personal autorizado.
  - Todo desarrollo antes de su pase a producción debe ser revisado, para asegurar que se cumplan con los estándares establecidos por la Oficina de Tecnologías de la Información y Estadística.
  - El pase a producción debe ser ejecutado por el responsable autorizado de la Oficina de Tecnologías de la Información y Estadística, quien llevará un

control de los pases efectuados y/o actualizaciones de los sistemas de información en un registro o bitácora.

- Control del sistema de información en producción: se deben formular y poner en práctica procedimientos para controlar la implementación del sistema de información en el ambiente de producción.

g. **Control de cambios en los sistemas de información**

- El control, registro y monitoreo de los cambios de los sistemas de información de la BNP debe ser supervisado y registrado por el responsable designado por la Oficina de Tecnologías de la Información y Estadística.
- El proceso de control de cambios debe considerar la implementación de un procedimiento de control de cambios.
- La Oficina de Tecnologías de la Información y Estadística debe efectuar revisiones periódicas de los sistemas de información en el ambiente de producción, a fin de asegurar que sólo se hayan efectuado los cambios autorizados.

6.8. Políticas para las relaciones con los/as prestadores/as de servicios

6.8.1. Objetivos

- Mantener la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso los/as prestadores/as de servicios. .
- La BNP debe verificar la implementación de los acuerdos de entrega de servicios, monitorear su cumplimiento con los estándares y gestionar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados.

6.8.2. Alcance

Estas políticas deben ser aplicables a los/as prestadores/as de servicios, que tengan alguna relación con la BNP, bien sea de tipo legal, contractual o de cualquier otra índole no laboral y que en razón de ésta, tengan acceso a información, sistemas de información, centros de datos, redes de telecomunicaciones o tecnologías de información de propiedad de la BNP.

6.8.3. Políticas

- Los/as prestadores/as de servicios que contemplen la gestión, transformación o transmisión de información deben conocer, aceptar y cumplir las políticas de seguridad de la información definidas por el SGSI.
- Para el acceso a cualquier tipo de información o sistema de información, los/as prestadores/as de servicios deberán suscribir una declaración de confidencialidad con el fin de reducir los riesgos de divulgación de información con carácter confidencial.
- En los contratos suscritos con prestadores/as de servicios se deben establecer y acordar los requisitos de seguridad que debe cumplir el/la prestador/a de servicios para poder tener acceso, procesar, almacenar, comunicar información de la BNP o para el suministro de componentes de infraestructura tecnológica a la BNP. En los acuerdos se deben incluir las medidas necesarias para el tratamiento de los riesgos de seguridad de la información derivados de las actividades realizadas por el/la

prestador/a de servicios. Los acuerdos deben ser formalizados antes del inicio de las actividades con el/la prestador/a de servicios.

- Los/as prestadores/as de servicios solo deben tener acceso a la información, sistemas de información o instalaciones que son indispensables para el cumplimiento de sus objetos contractuales.

- Al finalizar sus contratos, los/as prestadores/as de servicios deben efectuar la devolución de información o activos de información de propiedad de la BNP que estuvieron bajo su responsabilidad y procurar la destrucción o borrado seguro de información confidencial conocida en razón de su actividad.

- Los/as prestadores/as de servicios deben cumplir con la reglamentación en materia de propiedad intelectual, incluido pero no limitado al uso de información y sistema de información.

- Los/as prestadores/as de servicios no están autorizados para utilizar los recursos de información y tecnológico de la BNP para propósitos diferentes a los necesarios para el cumplimiento del objeto contractual suscrito.

- No está autorizada la utilización de equipos informáticos dentro de las redes de comunicaciones de la BNP que no cumplan con los controles de seguridad especificados por el SGSI de la BNP.

- No está autorizada la ejecución de cambios sobre la infraestructura tecnológica de la BNP sin contar con la autorización formal y expresa del responsable de la Oficina de Tecnologías de la Información y Estadística.

- No está autorizada la modificación o desactivación de los controles de seguridad instalados en los componentes de información y tecnología de la BNP sin contar con autorización del responsable del órgano de la BNP que utiliza el recurso informático.

- Los responsables de los órganos de la BNP deben evaluar periódicamente los riesgos que se identifiquen sobre la contratación de servicios de procesamientos de información con prestadores/as de servicios. Los resultados de la evaluación de riesgos deben generar propuestas de mecanismos de control que mitiguen los impactos de los riesgos identificados.

6.9. Políticas para la gestión de incidentes de seguridad de la información

6.9.1. Objetivos

- Asegurar que los eventos y debilidades de seguridad de la información asociados a los sistemas de información sean comunicados en forma adecuada, siguiendo los procedimientos correspondientes, permitiendo implementar una eficiente acción correctiva.

- Implementar procedimientos que contengan un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información.

6.9.2. Alcance

Estas políticas deben ser cumplidas por los/as usuarios/as de los distintos órganos de la BNP, y por los/as prestadores/as de servicios. .

6.9.3. **Políticas**

- Los incidentes relativos a la seguridad de la información deben comunicarse al/a la Oficial de Seguridad de la Información, y debe establecerse un proceso formal para la comunicación y tratamiento de los incidentes, a través de un procedimiento de gestión de incidentes de seguridad de la información.

- Los/as usuarios/as y los/as prestadores/as de servicios deben conocer el proceso para comunicar los incidentes de seguridad de la información, y deben informar de los mismos tan pronto como sea posible al/a la Oficial de Seguridad de la Información.

- Podrían ser considerados como incidentes de seguridad de la información para la BNP, los siguientes hechos:

    - Pérdida de acervo documental y bibliográfico de la BNP.
    - Acceso no autorizado a los repositorios y bóveda de la BNP.
    - Pérdida de servicio, equipos o instalaciones (disponibilidad de los servicios de la Oficina de Tecnologías de la Información y Estadística).
    - Errores humanos en uso de los sistemas.
    - Incumplimientos de políticas, normas y/o procedimientos sobre seguridad de la información.
    - Cambios no controlados en los sistemas (software y hardware) y servicios.
    - Accesos no autorizados a los sistemas de información y/o aplicativos.
    - Ataques por software de tipo malicioso (*malware*).
    - Correos fraudulentos (*phishing*) solicitando información del/de la usuario/a.
    - Pérdida o fuga de información (en formato físico o lógico).
    - Uso inadecuado del correo electrónico.
    - Detección de vulnerabilidades de la seguridad de red informática.

- Los/as usuarios/as y los/as prestadores/as de servicios deben conocer su responsabilidad respecto a la comunicación de eventos de seguridad de la información y el proceso para informarlos con prontitud a través de un flujo adecuado para garantizar que, el/la usuario/a o el/la prestador/a de servicios que comunica los incidentes, sea notificado/a de los resultados una vez que el tema haya sido resuelto.

- Reportados los incidentes de seguridad de la información a las partes correspondientes, se debe proceder al seguimiento detallado de dichos incidentes, los cuales serán investigados por la Oficina de Tecnologías de la Información y Estadística y la Oficina de Administración; y, de acuerdo al tipo de incidente se determinarán la severidad de los mismos. Ello se debe encontrar definido en el procedimiento de gestión de incidentes de seguridad de la información.

- Los incidentes de los controles serán corregidos mediante acciones específicas del Comité de Gestión de Seguridad de la Información.

- La determinación de la falta y la acción disciplinaria a la que podrían ser sometidos/as los/as usuarios/as se realizará acorde al marco normativo vigente.

- Periódicamente, el/la Oficial de Seguridad de la Información deberá analizar las actividades realizadas y estudiar posibles mejoras o cambios que puedan efectuarse ante futuros incidentes, previniendo la recurrencia de los mismos y evitando que estos se transformen en problemas. Para ello, se deberá realizar un análisis exhaustivo a fin de corregir la situación.

- Este análisis deberá aportar información para poder actuar conforme a las siguientes medidas:

    - Correctivas: para apoyar a la solución del incidente.
    - Preventivas: para evitar la ocurrencia del mismo o emprender oportunidades de mejora que puedan disminuir la situación de riesgos actual.

6.10. Políticas de los aspectos de seguridad de la información en la gestión de continuidad del negocio

6.10.1. Objetivos

- Reaccionar a la interrupción de servicios de la entidad y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres que afecten la infraestructura de los mismos.

- Documentar las actividades de recuperación de la operatividad y el servicio ante un incidente o evento severo.

- Documentar los planes y procedimientos de recuperación necesaria e indispensable para recuperar las operaciones y los servicios, que ofrece la BNP, en el tiempo definido.

6.10.2. Alcance

Estas políticas deben ser cumplidas por los/as usuarios/as de los distintos órganos de la BNP.

6.10.3. Políticas

a. **Seguridad de la información en el proceso de gestión de la continuidad del negocio**

- La BNP debe elaborar el Plan de Recuperación Tecnológica, el cual se desarrolla a raíz de la necesidad de mantener la disponibilidad ante una situación de contingencia severa que amenace paralizar totalmente los servicios informáticos de la entidad. Esto se puede hacer paulatinamente en un proceso a largo plazo en caso no se cuente con los recursos necesarios.

- El Plan de Recuperación Tecnológica se activará en escenarios de desastres catastróficos, y que imposibilite la operación normal de entrega de servicios de TI desde la Oficina de Tecnologías de la Información y Estadística.

b. **Continuidad de los servicios y evaluación de riesgos**

- Los eventos que pueden causar interrupciones a los servicios de la entidad deben ser identificados, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la continuidad de los servicios.

- En el análisis de impacto se deben identificar los procesos que se afectarían y valorar el impacto en función a la criticidad de estos. Asimismo, se debe identificar el tiempo objetivo de recuperación y el punto objetivo de recuperación en el cual la BNP retornará a realizar operaciones y servicios.

    - El Tiempo Objetivo de Recuperación (RTO), se refiere al tiempo disponible para recuperar los servicios de TI.

- El Punto Objetivo de Recuperación (RPO) se refiere a la magnitud de pérdida de datos medida en términos de un período de tiempo que puede ser tolerado.

c. **Redacción e implantación del plan de continuidad que incluyen la seguridad de la información**

- El Plan de Recuperación Tecnológica debe asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas por los procesos de la BNP, tras la interrupción o la falla de sus procesos críticos.

- Asimismo, dentro del Plan de Recuperación Tecnológica se deben considerar los tiempos de recuperación y de la estrategia de recuperación por cada sistema de información (aplicaciones y plataformas críticas) que pueden afectar directamente a la BNP. En base a los resultados podemos determinar no sólo la criticidad sino también la priorización y los esfuerzos de recuperación ante una situación de desastre.

d. **Marco de planificación para la continuidad del negocio**

- Es necesario establecer el marco bajo el cual se desarrollará y ejecutará el Plan de Recuperación Tecnológica. Para ello, se han definido los siguientes lineamientos:
  - El Plan de Continuidad se ejecutará únicamente cuando se determine que el tiempo de espera para la reanudación de los procesos exceda el tiempo máximo de indisponibilidad tolerable (MTD); y, por lo tanto, afecte negativamente al servicio en el centro de información principal de la BNP.
  - El Plan de Recuperación Tecnológica debe contar con un procedimiento de respaldo y recuperación de información que permita recuperar la misma.

- La estrategia de recuperación de la BNP permitirá restablecer, dentro de la ventana de tiempo de recuperación definida, las operaciones de la entidad minimizando el impacto del evento.

e. **Prueba, mantenimiento y reevaluación del plan de continuidad**

- El Plan de Recuperación Tecnológica debe ser probado regularmente para asegurar su actualización y eficiencia.

- Las pruebas del plan deben asegurar que todos los miembros del equipo de recuperación y otro personal relevante estén capacitados y conozcan sus responsabilidades para la continuidad de los servicios. Todos deben saber su rol cuando el plan sea invocado.

- El calendario de pruebas del Plan de Recuperación Tecnológica debe indicar cómo y cuándo probar cada procedimiento del plan.

f. **Redundancia**

- Considerar los componentes o arquitecturas redundantes cuando no se pueda garantizar el nivel de disponibilidad requerido por las actividades de la entidad a través de arquitecturas típicas o los sistemas existentes se demuestren insuficientes.

- Se deben probar los sistemas de información redundantes para garantizar que la conmutación funcione adecuadamente.

- Implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.

6.11. Políticas de cumplimiento

6.11.1. Objetivo

- Cumplir con las legislaciones, regulaciones, requerimientos contractuales y cualquier requerimiento de seguridad de la información.

- Asegurar el cumplimiento de lo establecido por el SGSI.

6.11.2. Alcance

Estas políticas deben ser cumplidas por los/as usuarios/as de los distintos órganos de la BNP.

6.11.3. Políticas

a. **Cumplimiento con los requisitos legales**

- Todas las legislaciones, regulaciones y requerimientos contractuales deben ser identificados, y deben estar documentados para su aplicación en tecnologías de la información de la BNP.

- Toda la información financiera, de impuestos y registros legales debe ser retenida por un período de al menos diez (10) años, mientras que el resto de información debe ser retenida por un período de al menos cinco (5) años.

- El personal de la BNP no debe destruir o eliminar registros o información importante, sin la aprobación respectiva de los propietarios de la información.

b. **Uso de software licenciado**

- El/La responsable de la Oficina de Tecnologías de la Información y Estadística debe velar porque todo el software de la BNP cuente con la respectiva licencia de uso. Cada vez que se formule un requerimiento de compra de un equipo de cómputo este debe considerar el costo de licencia del sistema operativo y los mínimos requerimientos de software para el desempeño de las labores de quien tenga asignado el equipo de cómputo.

- El personal de la Oficina de Tecnologías de la Información y Estadística debe evaluar y aprobar las solicitudes de software. Las solicitudes de software deben contar con la justificación necesaria indicando su frecuencia de uso y ser autorizadas por el responsable del órgano donde labora el/la usuario/a.

c. **Protección de datos y privacidad de la información personal**

Se deben implementar los controles necesarios que permitan asegurar los datos personales de los/as usuarios/as, en concordancia con la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento.

d. **Prevención de mal uso de los recursos de procesamiento de información**

Se debe cumplir con las disposiciones establecidas en el Reglamento Interno de los/as Servidores/as Civiles de la Biblioteca Nacional del Perú sobre el buen uso de los bienes.

e. **Revisiones de la política de seguridad y de la conformidad técnica**

- Los/as responsables de los órganos de la BNP deben asegurar que se cumplan todos los lineamientos y procedimientos de seguridad de la información establecidos en la entidad.
- Los/as usuarios/as que hagan mal uso de los recursos de tecnologías de la información podrían ser sancionados según la gravedad de la falta cometida y de conformidad con la normatividad aplicable.
- El/La Oficial de Seguridad de la Información deberá evaluar las Políticas de Seguridad de la Información implementadas en la BNP, una vez al año o cuando sea solicitado por el Comité de Gestión de Seguridad de la Información.
- El/La Oficial de Seguridad de la Información debe programar la realización de pruebas de comprobación técnica (pruebas de intrusión y análisis de vulnerabilidades) a cargo de especialistas externos para verificar que se han implementado correctamente los controles de seguridad definidos para el hardware y software.

7. ANEXOS

7.1. Anexo 01: Declaración de confidencialidad y no divulgación de información con usuarios/as.

7.2. Anexo 02: Declaración de confidencialidad y no divulgación de información con prestadores/as de servicios.

BIBLIOTECA NACIONAL DEL PERÚ V°B° Eduardo Rondal OTIE

BIBLIOTECA NACIONAL DEL PERÚ V°B° Augusto Fernandini OPP

BIBLIOTECA NACIONAL DEL PERÚ V°B° Eduardo Ulloa OPP EMO

BIBLIOTECA NACIONAL DEL PERÚ Oficial de Seguridad de la Información

BIBLIOTECA NACIONAL DEL PERÚ V°B° Gerald Benavente Q. Jefe E.T. Log. y C.P. Oficina de Administración

Anexo 01: Declaración de confidencialidad y no divulgación de información con usuarios/as.

El/La USUARIO/A se obliga a mantener y guardar estricta reserva y absoluta confidencialidad sobre las características, términos y condiciones de la presente Declaración de Confidencialidad y no Divulgación de Información.

El/La USUARIO/A se compromete a respetar y aplicar, en la ejecución del servicio de la presente declaración, la política, lineamientos, procedimientos, estándares y controles de seguridad de la información establecidos por la Biblioteca Nacional del Perú, los mismos que declara conocer y aceptar.

El/La USUARIO/A deberá proteger los activos de información la Biblioteca Nacional del Perú (Información física y digital, Software, Hardware, entre los principales) del acceso no autorizado, pérdida, modificación y/o destrucción, falsificación, robo, uso indebido y/o divulgación no autorizada.

El/La USUARIO/A se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos, datos e información la Biblioteca Nacional del Perú a los que tenga acceso en ejecución de la presente declaración. Se entiende que la obligación asumida por el/la USUARIO/A está referida no sólo a los documentos e información señalados como "confidenciales" sino a todos los documentos, datos e información que en razón de la presente declaración o vinculado con la ejecución del mismo, pueda ser conocida por cualquier medio por el/la USUARIO/A. En consecuencia, el/la USUARIO/A deberá abstenerse de divulgar tales documentos, conversaciones, datos, acuerdos de reuniones y comentarios que, como parte de su función, tome conocimiento, sea en forma directa o indirecta.

El/La USUARIO/A solo podrá revelar al personal que estrictamente sea necesario para la realización de las actividades materia de la presente declaración, los documentos, datos e información a los que se refiere al párrafo precedente.

En el caso que el/la USUARIO/A fuera requerido/a por alguna autoridad administrativa y/o judicial para revelar la información y/o documentación a la que se refiere la presente declaración, deberá notificar anticipadamente a la Biblioteca Nacional del Perú para que éste adopte las medidas que considere necesarias para proteger la confidencialidad de la información.

Se deja expresamente establecido que el deber de confidencialidad opera desde la fecha de suscripción de la presente declaración y se mantendrá vigente incluso hasta cinco (5) años posteriores a la extinción del mismo.

El/La USUARIO/A se compromete a devolver todo activo (software, documentación, equipos, tarjetas de acceso, entre los principales) que le haya proporcionado la Biblioteca Nacional del Perú para el desempeño de sus funciones, al momento de la resolución o término de su vínculo con la entidad, sin que sea necesario requerimiento alguno.

Cualquier incumplimiento de las obligaciones que constan en la presente declaración, intencionadamente o por negligencia, podría conllevar a la aplicación de sanciones disciplinarias correspondientes por parte de la Biblioteca Nacional del Perú.

FIRMA DEL/DE LA USUARIO/A:
NOMBRE DEL/DE LA USUARIO/A: .....
DNI DEL/DE LA USUARIO/A: .....

Anexo 02: Declaración de confidencialidad y no divulgación de información con prestadores/as de servicios.

Suscribe la presente Declaración de Confidencialidad y No Divulgación de Información:

<Nombres y apellidos o Razón Social>, con Registro Único de Contribuyente N° <número de RUC>, con domicilio <domicilio>, debidamente representado por el <Representante Legal>, identificado con DNI N° <DNI representante> (en adelante "EL CONTRATISTA"); bajo los términos y cláusulas siguientes:

PRIMERA: OBJETO
EL CONTRATISTA se compromete a tratar con estricta confidencialidad, a partir de la fecha de suscripción de esta declaración, tanto la información como las labores que desarrolle.

SEGUNDA: CONDICIONES
2.1. EL CONTRATISTA se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos e información (datos, registros, productos, equipos, lineamientos, procedimientos, estándares, metodologías, estudios, procesos, guías, documentos, topología de red, números telefónicos, direcciones IP, asignaciones de puertos, licencias de software, código fuente de sistemas de información, configuraciones, claves o credenciales, comunicaciones electrónicas) de la Biblioteca Nacional del Perú a los que tenga acceso en ejecución del contrato u orden de servicio. Se entiende que la obligación asumida por EL CONTRATISTA está referida no solo a los documentos e información señalada como "confidenciales" sino a todos los documentos e información que, en razón de la presente declaración, pueda ser conocida por cualquier medio. En consecuencia, EL CONTRATISTA deberá abstenerse de divulgar tales documentos e información, sea en forma directa o indirecta. EL CONTRATISTA conviene en que toda la información suministrada en virtud de esta declaración es confidencial y de propiedad la Biblioteca Nacional del Perú.

2.2. EL CONTRATISTA solo podrá revelar al personal que estrictamente sea necesario para la realización de las actividades materia del contrato u orden de servicio, los documentos e información a los que se refiere el numeral precedente. Asimismo, EL CONTRATISTA se obliga a tomar las medidas y precauciones razonables para que sus trabajadores, directores, accionistas, proveedores y en general, cualquier persona que tenga relación con EL CONTRATISTA no divulgue a ningún tercero los documentos e información a los que tenga acceso, haciéndose responsable por la divulgación que se pueda producir y asumiendo el pago de la indemnización por daños y perjuicios que la autoridad competente determine.

2.3. EL CONTRATISTA no debe destinar o utilizar los datos personales con una finalidad distinta a la autorizada por el titular del banco de datos personales o responsable del tratamiento. Además, EL CONTRATISTA se compromete a tratar los datos personales con la finalidad exclusiva de la realización del servicio. Una vez realizada la prestación del servicio, EL CONTRATISTA se compromete a destruir los datos personales proporcionados por la Biblioteca Nacional del Perú, así como, el resultado de cualquier elaboración de los mismos y los soportes o documentos en que se halle recogida la información o, en su caso, a devolvérselos a la Biblioteca Nacional del Perú en función de la decisión tomada por la misma en cada caso.

2.4. EL CONTRATISTA se obliga a utilizar los datos que facilite la Biblioteca Nacional del Perú única y exclusivamente para los fines de la presente declaración y a guardar secreto profesional respecto a todos los datos de carácter personal que conozca y a los que tenga acceso durante la realización del contrato de prestación de servicios. Igualmente, se obliga a custodiar e impedir el acceso a los datos de carácter personal a cualquier tercero ajeno a la presente declaración.

2.5. La obligación de confidencialidad establecida en la presente Declaración de Confidencialidad y No Divulgación de Información seguirá vigente incluso luego de la terminación del contrato u orden de servicio de acuerdo a lo especificado en la cláusula quinta de la presente declaración.

2.6. EL CONTRATISTA se compromete a devolver todo el material que le haya proporcionado la Biblioteca Nacional del Perú al momento de resolución o término del contrato u orden de servicio, sin que sea necesario de éste se lo requiera.
El incumplimiento probado de las obligaciones que asume EL CONTRATISTA en virtud de la presente Declaración de Confidencialidad y No Divulgación de Información podría constituir causal de resolución contractual, sin perjuicio de las acciones legales correspondientes.

TERCERA: DEVOLUCIÓN DE INFORMACIÓN ENTREGADA
La información confidencial entregada de forma tangible no deberá ser reproducida por EL CONTRATISTA, a menos que se cuente con expresa y escrita autorización de la Biblioteca Nacional del Perú.
A solicitud de la Biblioteca Nacional del Perú, EL CONTRATISTA deberá devolver toda la información confidencial, y cualquiera de las copias o datos derivados del mismo dentro de los diez (10) días posteriores de tal pedido. La Biblioteca Nacional del Perú podrá solicitar a EL CONTRATISTA destruir cualquiera de las notas, memorándums, documentos, o datos derivados que sean solicitados.

CUARTA: COMUNICACIONES
Toda comunicación que deba ser cursada a la Biblioteca Nacional del Perú se entregará en Mesa de Partes de la entidad, ubicada en Avenida De la Poesía 160, distrito de San Borja, provincia y departamento de Lima, y para EL CONTRATISTA se entregará en el domicilio consignado en la parte introductoria del presente documento. En caso de modificación del domicilio, el nuevo domicilio deberá ser comunicado mediante carta notarial.

QUINTA: PLAZO
El deber de confidencialidad opera desde la fecha de suscripción de la presente declaración y seguirá vigente incluso luego de la terminación del contrato u orden de servicio, hasta por cinco (05) años.

SEXTA: NATURALEZA
La presente declaración es de naturaleza exclusivamente civil, por lo que en todo aquello no previsto en este documento será aplicable lo establecido en la legislación peruana que regule la materia, tal como el Código Civil.

SÉTIMA: ALCANCE DE LA DECLARACIÓN
Cualquier referencia al aspecto de confidencialidad que se inserte en las cláusulas del contrato u orden de servicio se entenderán como complementarias a la presente declaración.

OCTAVA: SOLUCIÓN DE CONFLICTOS
Para todos los efectos de la presente declaración, ante cualquier disputa, conflicto, controversia o reclamo que pudiera surgir sobre la interpretación, ejecución o alcances de la presente declaración se resolverán, de conformidad con los reglamentos de conciliación y arbitraje, aplicando complementariamente lo que establece la Ley de Contrataciones del Estado o el Sistema Nacional de Arbitraje en lo que corresponde, a cuyas normas EL CONTRATISTA se somete.

Suscrito en la ciudad de Lima, el <día> de <mes> del <año>.

Firma y sello
EL CONTRATISTA