Resolución de Gerencia General

N° 028-2018-BNP/GG

Lima, 28 NOV 2018

VISTOS: el Informe Técnico N° 016-2018-BNP-GG-OSI de fecha 09 de octubre de 2018, de la Oficial de Seguridad de la Información; el Informe Técnico N° 003-2018-BNP-GG-OPP-EMO de fecha 13 de noviembre de 2018, del Equipo de Trabajo de Modernización de la Oficina de Planeamiento y Presupuesto; el Memorando N° 846-2018-BNP-GG-OPP de fecha 13 de noviembre de 2018, de la Oficina de Planeamiento y Presupuesto; y, el Informe Legal N° 256-2018-BNP-GG-OAJ de fecha 23 de noviembre de 2018, de la Oficina de Asesoría Jurídica, y;

CONSIDERANDO:

Que, el artículo 1 de la Resolución Ministerial N° 004-2016-PCM aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, el numeral 6.1.2 de la mencionada Norma Técnica Peruana señala respecto de la valoración del riesgo de seguridad de la información, lo siguiente:

"6.1.2 Valoración del riesgo de seguridad de la información
La organización debe definir y aplicar un proceso de valoración del riesgo de seguridad de la información que:

a) establezca y mantenga criterios de riesgo de seguridad de la información que incluyan;
   1) los criterios de aceptación de los riesgos; y
   2) los criterios para realizar valoraciones de riesgo de seguridad de la información;
b) asegure que las valoraciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables;
c) identifique los riesgos de seguridad de la información
   1) aplicando el proceso de valoración de riesgos de seguridad de la información para identificar riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad para la información dentro del alcance del sistema de gestión de seguridad de la información; e
   2) identificando a los propietarios de riesgos;
d) analice los riesgos de seguridad de la información:
   1) valorando las consecuencias potenciales que resultarían si los riesgos identificados en 6.1.2 c) 1) fueran a materializarse;
   2) valorando la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2.c) 1); y

3) determinando los niveles de riesgo;

e) evalúe los riesgos de seguridad de la información:

1) comparando los resultados del análisis de riesgo con los criterios de riesgo establecidos en 6.1.2.a); y

2) priorizando los riesgos analizados para el tratamiento de riesgos.

La organización debe retener información documentada sobre el proceso de valoración de riesgos de seguridad de la información."

Que, el numeral 6.1.3 de la mencionada Norma Técnica Peruana establece respecto del tratamiento de riesgos de seguridad de la información, lo siguiente:

"6.1.3 Tratamiento de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para:

a) seleccionar opciones de tratamiento de riesgos de seguridad de la información apropiadas, tomando en cuenta los resultados de la valoración de riesgos;

b) determinar todos los controles que son necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

(...)

c) Comparar los controles determinados en 6.1.3 b) con aquellos del Anexo A y verificar que no se ha omitido ningún control necesario;

(...)

d) producir una Declaración de Aplicabilidad que contenga los controles necesarios (...) y la justificación de las inclusiones ya sea que se implementen o no, así como la justificación de excluir controles del Anexo A;

e) formular un plan de tratamiento de riesgos de seguridad de la información; y

f) obtener la aprobación, por parte de los propietarios de riesgos, del plan de tratamiento de riesgos de la seguridad de la información y la aceptación de los riesgos residuales de la seguridad de la información.

La organización debe retener información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información."

Que, en atención a lo expuesto en los considerandos precedentes, a través del Informe Técnico N° 016-2018-BNP-GG-OSI de fecha 09 de octubre de 2018, la Oficial de Seguridad de la Información presentó la propuesta de la metodología para la identificación, análisis y evaluación de riesgos del Sistema de Gestión de Seguridad de la Información, indicando lo siguiente: *"De acuerdo a los numerales 6.1.2 y 6.1.3 Norma Técnica Peruana "NTP-ISO/IEC 27001:2014, se propone la Metodología para la identificación, análisis y evaluación de riesgos del Sistema de Gestión de Seguridad de la Información que permitirá gestionar adecuadamente los riesgos que se identifiquen en los activos de información y que son parte del Sistema de Gestión de Seguridad de la Información (SGSI) en la Biblioteca Nacional del Perú";*

Que, mediante Informe Técnico N° 003-2018-BNP-GG-OPP-EMO y Memorando N° 846-2018-BNP-GG-OPP, ambos de fecha 13 de noviembre de 2018, el Equipo de Trabajo de Modernización y la Oficina de Planeamiento y Presupuesto, emitieron opinión favorable respecto de la mencionada propuesta;

Que, el literal c) del numeral 1.1 del artículo 1 de la Resolución Jefatural N° 063-2018-BNP publicada el 12 de junio de 2018 en el Diario Oficial El Peruano dispone que, en materia de gestión administrativa, la Gerencia General tiene, entre otras facultades y atribuciones, la de: *"Aprobar*

Directivas, manuales de procedimientos y todo tipo de disposiciones internas vinculadas a la conducción de la institución";

Que, con el Informe Legal N° 256-2018-BNP-GG-OAJ de fecha 23 de noviembre de 2018, la Oficina de Asesoría Jurídica concluyó que resulta legalmente viable aprobar la referida propuesta;

Con el visado de la Oficial de Seguridad de la Información, de la Oficina de Planeamiento y Presupuesto; y, de la Oficina de Asesoría Jurídica;

De conformidad con lo dispuesto en la Resolución Ministerial Nº 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática; el Reglamento de Organización y Funciones de la Biblioteca Nacional del Perú, aprobado por Decreto Supremo N° 001-2018-MC; y, demás normas pertinentes;

SE RESUELVE:

Artículo 1.- APROBAR la Metodología para la identificación, análisis y evaluación de riesgos del Sistema de Gestión de Seguridad de la Información, 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

METODOLOGÍA IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código: SGSI-ME-01

Versión: 01

HOJA DE CONTROL DE CAMBIOS DEL DOCUMENTO				
Nro. de Cambio	Fecha de Cambio	Tipo[1]	Descripción del cambio	Responsable de modificación

BIBLIOTECA NACIONAL DEL PERU
Oficial de Seguridad de la Información

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

1. OBJETIVO

Establecer una metodología para la identificación, análisis y la evaluación de los riesgos de seguridad de la información para la Biblioteca Nacional del Perú.

2. ALCANCE

Es aplicable a la gestión de riesgos de seguridad de la información en los activos de información de aquellos procesos que forman parte del Sistema de Gestión de Seguridad de la Información – SGSI en la Biblioteca Nacional del Perú.

3. BASE NORMATIVA

3.1. Ley N° 30570, Ley General de la Biblioteca Nacional del Perú.
3.2. Ley N° 30034, Ley del Sistema Nacional de Bibliotecas.
3.3. Ley N° 29733, Ley de Protección de Datos Personales.
3.4. Decreto Supremo N° 001-2018-MC que aprueba el Reglamento de Organización y Funciones de la Biblioteca Nacional del Perú.
3.5. Decreto Supremo Nº 010-2017-MC que aprueba el Reglamento de la Ley N° 30570, Ley General de la Biblioteca Nacional del Perú.
3.6. Decreto Supremo Nº 002-2014-MC que aprueba el Reglamento de la Ley N° 30034, Ley del Sistema Nacional de Bibliotecas.
3.7. Decreto Supremo N° 003-2013-JUS que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
3.8. Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

4. REFERENCIAS

4.1. Procedimiento inventario, etiquetado y tratamiento de activos de la información del Sistema de Gestión de Seguridad de la Información (SGSI-PR-02).

5. DEFINICIONES Y ABREVIATURAS

5.1. **Aceptación del riesgo**: Decisión informada para aceptar un riesgo particular.
5.2. **Activo de información**: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la entidad.
5.3. **Alcance**: Ámbito de la BNP 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.
5.4. **Amenaza**: Posible causa de un incidente no deseado, que puede resultar en daño a un sistema u organización. Es un evento que potencialmente puede causar daño.
5.5. **Análisis de riesgos**: Proceso para comprender la naturaleza del riesgo, y para determinar el nivel de riesgo.
5.6. **Análisis de riesgos cualitativo**: Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.

5.7. **Análisis de riesgos cuantitativo**: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.
5.8. **Autenticación**: Provisión de seguridad de que una característica alegada de una entidad es correcta.
5.9. **Confidencialidad**: Propiedad que la información no esté disponible o se dé a conocer a personas no autorizadas, entidades o procesos.
5.10. **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.
5.11. **Custodio de activo de información:** Identifica al órgano que tiene la responsabilidad de mantener los niveles de protección adecuados en base a las especificaciones dadas por el propietario del activo de información.
5.12. **Declaración de aplicabilidad**: (Statement of Applicability; SoA). Documento que enumera los controles aplicados por el SGSI de la entidad -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la Norma Técnica Peruana vigente.
5.13. **Disponibilidad**: Propiedad de ser accesible y utilizable a petición por una entidad autorizada.
5.14. **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.
5.15. **Evento**: Ocurrencia o cambio de un conjunto particular de circunstancias.
5.16. **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.
5.17. **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.
5.18. **Gestión de riesgos**: Actividades coordinadas para dirigir y controlar la entidad con respecto al riesgo.
5.19. **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.
5.20. **Identificación de riesgos**: Proceso de encontrar, reconocer y describir los riesgos.
5.21. **Integridad**: Propiedad que busca garantizar una información exacta y libre de errores, la misma que puede ser modificada bajo autorización.
5.22. **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.
5.23. **Mejora continua**: Actividad recurrente para mejorar el rendimiento.
5.24. **Nivel de riesgo**: Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad.
5.25. **No repudio**: Capacidad para demostrar la ocurrencia de un evento o acción que se atribuye y sus entidades de origen.
5.26. **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.

BIBLIOTECA NACIONAL DEL PERÚ Oficial de Seguridad de la Información

5.27. **Política de seguridad:** Documento que establece el compromiso de la Alta Dirección y el enfoque de la BNP en la gestión de la seguridad de la información. Según la ISO/IEC 27002 es la intención y dirección general expresada formalmente por la Alta Dirección.

5.28. **Probabilidad:** Es la posibilidad de que un evento cualquiera ocurra o no. A mayor probabilidad del evento existe más posibilidad de que ocurra, es decir, existen buenas razones para creer que sucederá.

5.29. **Procedimiento:** Forma especificada para llevar a cabo una actividad o un proceso.

5.30. **Proceso de gestión de riesgos**: La aplicación sistemática de políticas, procedimientos y prácticas para las actividades de comunicación, consultoría, estableciendo el contexto y la identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgo.

5.31. **Propietario de activo de información**: Identifica al órgano que tiene responsabilidad aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

5.32. **Propietario de riesgo**: La persona u órgano que tiene la responsabilidad y la autoridad para administrar un riesgo.

5.33. **Registro:** Documento que presenta resultados obtenidos o proporciona evidencias de actividades desempeñadas.

5.34. **Riesgo de seguridad de la información:** Posibilidad que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la BNP.

5.35. **Riesgo efectivo**: Es la medida del daño probable causado por una amenaza que se materializa en un activo.

5.36. **Riesgo residual**: Riesgo que queda después del tratamiento del riesgo.

5.37. **Tratamiento de riesgos**: Proceso para modificar el riesgo.

5.38. **Valoración de riesgos**: Proceso completo de análisis y evaluación de riesgos.

5.39. **Vulnerabilidad:** Debilidad de un activo o de control que puede ser explotado por una o más amenazas.

5.40. **Usuario/a:** Es quien independientemente del régimen laboral o modalidad contractual se vincula a la entidad.

5.41. **BNP:** Biblioteca Nacional del Perú.

5.42. **CID**: Acrónimo español de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.

5.43. **SGSI**: Sistema de Gestión de la Seguridad de la Información. Es la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).

6. RESPONSABILIDAD

6.1. Los propietarios de los activos de información son responsables de lo siguiente:

- Dar cumplimiento a este procedimiento.
- Promover la participación activa de los/as usuarios/as en la identificación, análisis y evaluación de riesgos de seguridad de la información.
- Revisar y dar la conformidad a la matriz de riesgos.

6.2. El Comité de Gestión de Seguridad de la Información es responsable de lo siguiente:

- Aprobar el resultado de la evaluación de riesgos.

6.3. El Oficial de Seguridad de la Información es responsable de lo siguiente:

- Verificar el cumplimiento del presente documento.

- Liderar los talleres a desarrollarse para la identificación, análisis y evaluación de riesgos de seguridad de la información.
- Compilar información remitida por los propietarios de los activos de información relacionada a la identificación, análisis y evaluación de riesgos de seguridad de la información.
- Presentar a los responsables del proceso el resultado del análisis y evaluación de riesgos.
- Presentar al Comité de Gestión de Seguridad de la Información el resultado del análisis y evaluación de riesgos para su aprobación.

7. CONTENIDO

El proceso de análisis de riesgos está sujeto a métodos de valorización cualitativos y está orientado a los activos de información, que soportan los procesos de la BNP.

7.1. Identificación de activos de información

La identificación y valorización de activos de información, se realizará según lo indicado en el *Procedimiento de Inventario, Etiquetado y Tratamiento de Activos de Información (SGSI-PR-02)* y el *Formato Inventario de Activos de Información (SGSI-FO-08)*.

Una vez valorizados los activos de información, solo se realizará el análisis de riesgo a los activos de información cuyo valor sea **alto**, los mismos que se incluirán en el *Formato Análisis y Evaluación de Riesgos (SGSI-FO-09)*.

7.2. Identificación de las amenazas

Para la identificación de las amenazas se utilizará la tabla de amenazas y vulnerabilidades (ver Anexo 05 - Tabla de Amenazas).

7.3. Identificación de vulnerabilidades

Para la identificación de las vulnerabilidades se utilizará la tabla de amenazas y vulnerabilidades (ver Anexo 06 - Tabla de Vulnerabilidades).

7.4. Determinación del impacto

Para determinar cómo la amenaza afecta la preservación de la confidencialidad, integridad y disponibilidad (CID) del activo de información, se evaluará cada uno de los criterios.

Activo	Amenaza	Vulnerabilidad	¿Qué afecta en los activos de información?				Riesgo Efectivo
			C	I	D	Valor CID	Impacto

7.4.1. Evaluación del criterio CID

Primero se evaluará cada uno de los criterios CID, se tomarán los siguientes valores:

a. Tabla de valorización de confidencialidad

Valor	Clasificación	Definición	Consecuencia
3	**Alta**	Es la información o recurso que debe ser divulgada sólo a fuentes autorizadas, controladas y debidamente identificadas. Debe ser modificada y leída por un grupo reducido de personas autorizadas y claramente identificadas.	La divulgación no autorizada produce: • Pérdida de la imagen institucional. • Uso malicioso en contra de la BNP. • Pérdidas financieras que no pueden ser absorbidas por la BNP. • Demandas legales que dañan la imagen y confianza pública de la BNP.
2	**Media**	Es la información que debe ser divulgada sólo al personal de los órganos que la manejan y modificada sólo por personas autorizadas e individualizadas.	La divulgación no autorizada produce: • Uso malicioso en contra de la imagen o situaciones puntuales. • Pérdidas financieras que pueden ser absorbidas por la BNP. • No se producen demandas legales.
1	**Baja**	Es la información que puede ser divulgada al público en general, pero que sólo puede ser modificada por personas autorizadas.	La divulgación no autorizada no representa perjuicio para la BNP.

BIBLIOTECA NACIONAL DEL PERÚ
Oficial de Seguridad de la Información

b. Tabla de valorización de integridad

Valor	Clasificación	Criterio	Consecuencia
3	**Alta**	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de gran magnitud.	La falta de integridad produce daños de gran magnitud los que se pueden expresar como: • Pérdidas económicas (pérdida, incumplimiento de metas). • Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo más allá de lo estimado como manejable). • Daño de la imagen de la BNP (daño a nivel nacional e internacional que no se puede reparar en el corto plazo). • Pérdida de la confianza de los/as usuarios/as y del público en general.
2	**Media**	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de mediana magnitud.	La falta de integridad produce daños de mediana magnitud los que se pueden expresar como: • Pérdidas económicas (menor ganancia, incumplimiento de metas en menor escala). • Falla de los procesos informáticos (incapacidad de ejecutarlos por un periodo de tiempo que está en el límite superior de lo estimado como manejable). • Daño de la imagen de la BNP (daño a nivel nacional, se puede reparar en el corto plazo). • No se pierde la confianza de los/as usuarios/as ni del público en general.
1	**Baja**	Es la información o recurso que al ser modificado, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de pequeña magnitud.	La falta de integridad produce daños de pequeña magnitud los que se pueden expresar como: • Pérdidas económicas (no impacta las ganancias, se cumplen las metas). • Falla de los procesos informáticos (incapacidad de ejecutarlos por un período de tiempo pero este es manejable). • Daño de la imagen de la BNP (daño a nivel nacional que puede no ser percibido y se puede reparar prontamente). • No se pierde la confianza de los/as usuarios/as.

BIBLIOTECA NACIONAL DEL PERU Oficial de Seguridad de la Información

c. Tabla de valorización de disponibilidad

Valor	Clasificación	Definición	Consecuencia
3	**Alta**	Es información o activo de información indispensable para la continuidad de la BNP. El recurso principal y el alternativo no pueden faltar por un período prolongado de tiempo en horarios críticos.	La falta de disponibilidad por períodos prolongados produce: • Incumplimiento a los acuerdos de nivel de servicio. La transición entre el recurso principal y el alternativo no debe impactar el acuerdo de servicio. • Perjuicios legales que afectan la imagen de la BNP. • Perjuicios económicos que no pueden ser absorbidos por la BNP. • Problemas sindicales.
2	**Media**	La disponibilidad de la información es necesaria para la continuidad de la BNP, pero existen canales alternativos para contrarrestar una pérdida de disponibilidad en un tiempo razonable. El recurso principal y el alternativo pueden quedar fuera de servicio por un periodo mínimo de tiempo en horarios críticos.	La falta de disponibilidad produce: • Que los niveles de servicio acordados se puedan ver afectados en la transición entre el medio principal y el alternativo. • Perjuicios legales que no comprometen la imagen de la BNP. • Perjuicios económicos que pueden ser absorbidos por la BNP. • No hay problemas sindicales.
1	**Baja**	Es información o activos de información de apoyo o secundarios para la entidad. La información se encuentra duplicada en varias fuentes. Si no está disponible no compromete procesos operativos importantes.	La falta de disponibilidad produce: • Que los niveles de servicio acordados para los procesos operativos importantes, no se ven afectados. • Problemas administrativos y operativos no significativos. • Perjuicios económicos que no son significativos. • No hay perjuicios legales. • No hay problemas sindicales.

BIBLIOTECA NACIONAL DEL PERÚ
Oficial de Seguridad de la Información

7.4.2. **Valor CID**

Se calcula el valor CID de acuerdo a la siguiente tabla

a. Tabla de valorización

Aspecto de seguridad afectado por el riesgo			IMPACTO
C	I	D	
1	1	1	Insignificante
1	1	2	Leve
1	1	3	Mayor
1	2	1	Leve
1	2	2	Moderado
1	2	3	Mayor
1	3	1	Mayor
1	3	2	Mayor
1	3	3	Desastroso
2	1	1	Leve
2	1	2	Moderado
2	1	3	Mayor
2	2	1	Moderado
2	2	2	Moderado
2	2	3	Mayor
2	3	1	Mayor
2	3	2	Mayor
2	3	3	Desastroso
3	1	1	Mayor
3	1	2	Mayor
3	1	3	Desastroso
3	2	1	Mayor
3	2	2	Mayor
3	2	3	Desastroso
3	3	1	Desastroso
3	3	2	Desastroso
3	3	3	Desastroso

BIBLIOTECA NACIONAL DEL PERU
Oficial de Seguridad de la Información

7.4.3. Determinación del impacto en la BNP

Finalmente se determina el impacto de acuerdo a la siguiente tabla:

a. Tabla de valorización del impacto del riesgo

Nivel	Descripción	Impacto en la BNP
5	**Desastroso**	Impacta en forma severa en la BNP al punto de comprometer la confidencialidad o integridad de información crítica de la entidad o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por la entidad. El impacto es a toda la entidad y su efecto se siente en todo el personal involucrado.
4	**Mayor**	Impacta en forma grave a un órgano o servicio específico de la BNP, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves de la BNP por un tiempo considerable. Su efecto está limitado dentro de la BNP.
3	**Moderado**	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	**Leve**	El impacto es leve y se puede prescindir del mismo en un tiempo limitado.
1	**Insignificante**	No representa un impacto importante para la BNP.

7.5. Determinación de la probabilidad de ocurrencia

Finalmente se determina la probabilidad de ocurrencia.

Activo	Amenaza	Vulnerabilidad	¿Qué afecta en los activos de información?				Riesgo Efectivo	
			C	I	D	Valor CID	Impacto	Probabilidad

Para este caso utilizaremos los siguientes valores:

BIBLIOTECA NACIONAL DEL PERÚ
Oficial de Seguridad de la Información

Valor	Clasificación	Definición
1	**Remota**	El evento no ocurre nunca o casi nunca. Ha ocurrido al menos 1 vez al año.
2	**Aislada**	Si bien el evento puede ocurrir, el periodo entre uno y otro evento puede ser muy grande. Al menos 2 veces al año.
3	**Ocasional**	Es posible que ocurra el evento con una frecuencia baja. 3 o 4 veces al año.
4	**Recurrente**	Existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo pero la frecuencia no es alta. 1 vez al mes.
5	**Frecuente**	El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta. 1 vez a la semana o más.

7.6. Determinación del riesgo efectivo

Para determinar el riesgo efectivo se requiere obtener el impacto y la probabilidad de ocurrencia en un activo de información.

La codificación del riesgo será:

Rxy	
R	Riesgo
xy	Correlativo numérico del riesgo identificado

Activo	Amenaza	Vulnerabilidad	¿Qué afecta en los activos de información?				Riesgo Efectivo					Propietario del Riesgo
			C	I	D	Valor CID	Impacto	Probabilidad	Nivel de riesgo	Código del riesgo	Nombre de riesgo	

El propietario del riesgo es el mismo identificado como propietario del activo de información en el inventario de activos.

Con el valor obtenido del producto del impacto por la probabilidad obtenemos el riesgo, para esta actividad utilizaremos la Tabla de valorización del riesgo.

a. Tabla de valorización del riesgo

Tabla de Valorización de Riesgos					
Impacto		Probabilidad		Riesgo	
Desastroso	5	Frecuente	5	Inaceptable	25
Mayor	4	Frecuente	5	Inaceptable	20
Moderado	3	Frecuente	5	Importante	15
Leve	2	Frecuente	5	Moderado	10
Insignificante	1	Frecuente	5	Moderado	5
Desastroso	5	Recurrente	4	Inaceptable	20
Mayor	4	Recurrente	4	Importante	16
Moderado	3	Recurrente	4	Importante	12
Leve	2	Recurrente	4	Moderado	8
Insignificante	1	Recurrente	4	Tolerable	4
Desastroso	5	Ocasional	3	Importante	15
Mayor	4	Ocasional	3	Importante	12
Moderado	3	Ocasional	3	Moderado	9
Leve	2	Ocasional	3	Moderado	6
Insignificante	1	Ocasional	3	Tolerable	3
Desastroso	5	Aislada	2	Moderado	10
Mayor	4	Aislada	2	Moderado	8
Moderado	3	Aislada	2	Moderado	6
Leve	2	Aislada	2	Tolerable	4
Insignificante	1	Aislada	2	Admisible	2
Desastroso	5	Remota	1	Moderado	5
Mayor	4	Remota	1	Tolerable	4
Moderado	3	Remota	1	Tolerable	3
Leve	2	Remota	1	Admisible	2
Insignificante	1	Remota	1	Admisible	1

BIBLIOTECA NACIONAL DEL PERÚ
Oficial de Seguridad de la Información

b. Tabla mapa de exposición de los riesgos

Matriz Probabilidad – Impacto							
PROBABILIDAD	FRECUENTE	5	RIESGO MODERADO	RIESGO MODERADO	RIESGO IMPORTANTE	RIESGO INACEPTABLE	RIESGO INACEPTABLE
	RECURRENTE	4	RIESGO TOLERABLE	RIESGO MODERADO	RIESGO IMPORTANTE	RIESGO IMPORTANTE	RIESGO INACEPTABLE
	OCASIONAL	3	RIESGO TOLERABLE	RIESGO MODERADO	RIESGO MODERADO	RIESGO IMPORTANTE	RIESGO IMPORTANTE
	AISLADA	2	RIESGO ADMISIBLE	RIESGO TOLERABLE	RIESGO MODERADO	RIESGO MODERADO	RIESGO MODERADO
	REMOTA	1	RIESGO ADMISIBLE	RIESGO ADMISIBLE	RIESGO TOLERABLE	RIESGO TOLERABLE	RIESGO MODERADO
			1	2	3	4	5
			INSIGNIFICANTE	LEVE	MODERADO	MAYOR	DESASTROSO
			IMPACTO				

Los riesgos serán clasificados de acuerdo a niveles, según su grado de exposición, lo cual se muestra en la siguiente tabla:

Nivel de Riesgo		Descripción de las Consecuencias
Inaceptable	De 20 a 25	Puede afectar seriamente a la BNP, en términos de paralización de las operaciones, daño a la imagen de la BNP. Requiere acción correctiva inmediata más allá del tiempo tolerable, pérdidas considerables o demandas legales y daño considerable.
Importante	De 12 a 16	Puede afectar los niveles de operación y servicio de la BNP, incumplimiento de metas, y divulgación no autorizada de información fuera de la BNP. Requiere una acción correctiva sujeta a la discreción de la Alta Dirección en términos de plazos y compromisos.
Moderado	De 5 a 10	Afecta a los activos de información de soporte a los activos principales, puede afectar la disponibilidad en órganos específicos de la BNP. La divulgación no autorizada no representa perjuicio importante para la BNP. Su aceptación está sujeta a la revisión de la Alta Dirección.
Tolerable	De 3 a 4	No causa un efecto considerable en la BNP. Usualmente son aceptados sin revisión.
Admisible	De 1 a 2	El efecto para la BNP es insignificante. Usualmente no se les considera para la gestión de riesgos.

7.7. Tratamiento del riesgo

La BNP reconoce los siguientes niveles de riesgos:

- Inaceptable
- Importante
- Moderado
- Tolerable
- Admisible

Para la etapa de tratamiento del riesgo, se han considerado como **Aceptables** los riesgos definidos como:

- Moderado
- Tolerable
- Admisible

Aceptable, se da en el caso de quedar un riesgo "Admisible", "Tolerable" o "Moderado", para lo cual se acepta la pérdida probable generada por el riesgo por ser considerada mínima en comparación de implementar un control (Costo-Beneficio). Se podrían elaborar planes de contingencia para su respuesta.

Para los riesgos de nivel "Inaceptable" e "Importante" se procederán a evaluar las siguientes opciones de tratamiento de riesgo:

- Reducir o mitigar el riesgo: Implica tomar medidas o acciones de control encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).

- Evitar el riesgo: Es la alternativa ante un riesgo catastrófico e inminente y demasiado costoso de mitigar. Se logra cuando al interior del proceso se generan cambios sustanciales por mejoramiento o rediseño. Solo se puede evitar un riesgo si se elimina la actividad o la causa que lo origine.

- Transferir o compartir el riesgo: Implica trasladar el impacto negativo de una amenaza a un tercero. Transferir el riesgo implica trasladar a otra parte la responsabilidad de su gestión, (no elimina el riesgo).

Los mismos que se incluirán en el *Formato Plan de Tratamiento de Riesgos (SGSI-FO-10)*.

Cabe mencionar que durante la etapa de tratamiento de riesgos, cuando el costo de reducir el riesgo sea mayor, al costo del riesgo y/o al activo que lo produce, entonces también el riesgo se considera aceptable y se incluirán en el *Formato Aceptación de Riesgos (SGSI-FO-11)*.

La decisión sobre el tratamiento de un riesgo se realiza en cada ciclo de evaluación, la cual se realizará una vez al año o cuando ocurran cambios en los procesos del SGSI. Los planes de tratamiento de riesgo, son revisados con periodicidad no mayor a un año por parte del Comité de Gestión de Seguridad de la Información, los nuevos riesgos efectivos son medidos y comparados con los riesgos residuales estimados.

7.8. Declaración de aplicabilidad

Posterior al tratamiento de riesgos se desarrolla la declaración de aplicabilidad, una vez que se ha definido las opciones de tratamiento para los riesgos, la BNP debe aplicar medidas de control, es decir, indicar de qué manera serán modificados los riesgos, es aquí que se hace uso del *Formato Declaración de Aplicabilidad (SGSI-FO-12)*, en dicho documento se registran los controles de seguridad que son aplicables y si estos se encuentran operando o no. Así también, se debe justificar el por qué algunas medidas fueron excluidas.

8. REGISTROS

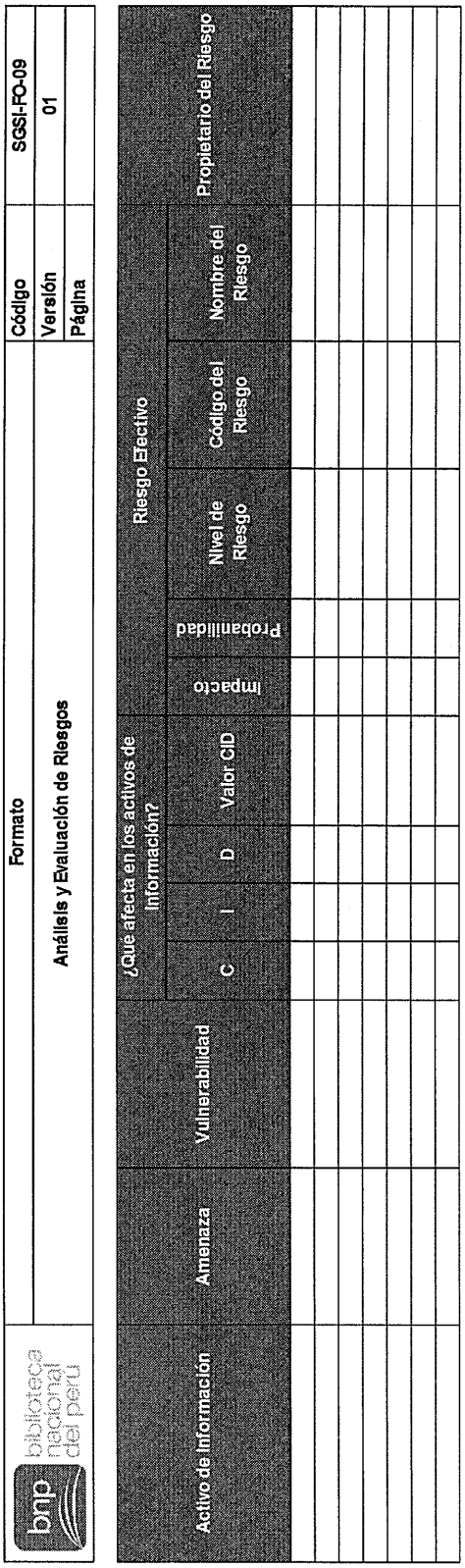
8.1. Formato Análisis y Evaluación de Riesgos (SGSI-FO-09).
8.2. Formato Plan de Tratamiento de Riesgos (SGSI-FO-10).
8.3. Formato Aceptación de Riesgos (SGSI-FO-11).
8.4. Formato Declaración de Aplicabilidad (SGSI-FO-12).

9. ANEXOS

9.1. Anexo 01: Formato Análisis y Evaluación de Riesgos.
9.2. Anexo 02: Formato Plan de Tratamiento de Riesgos.
9.3. Anexo 03: Formato Aceptación de Riesgos.
9.4. Anexo 04: Formato Declaración de Aplicabilidad
9.5. Anexo 05: Tabla de Amenazas
9.6. Anexo 06: Tabla de Vulnerabilidades

BIBLIOTECA NACIONAL DEL PERÚ
Oficial de Seguridad de la Información

Anexo 01: Formato Análisis y Evaluación de Riesgos



biblioteca nacional del perú	Formato	Código	SGSI-FO-09
	Análisis y Evaluación de Riesgos	Versión	01
		Página	

Activo de Información	Amenaza	Vulnerabilidad	¿Que afecta en los activos de información?				Riesgo Efectivo					
			C	I	D	Valor CID	Impacto	Probanilidad	Nivel de Riesgo	Código del Riesgo	Nombre del Riesgo	Propietario del Riesgo

Nombre y firma Presidente del CGSI

Nombre y firma del Propietario del Riesgo

Anexo 02: Formato Plan de Tratamiento de Riesgos

	Formato	Código	SGSI-FO-10
bnp biblioteca nacional del perú	Plan de Tratamiento de Riesgos	Versión	01
		Página	

Código del Riesgo	Nombre del Riesgo	Propietario del Riesgo	Activo de Información	Control Referencia	Acción a realizar	Plazo de Implementación	Responsable

Anexo 03: Formato Aceptación de Riesgos

	Formato	Código	SGSI-FO-11
bnp biblioteca nacional del perú	Aceptación de Riesgos	Versión	01
		Página	

El Comité de Gestión de Seguridad de la Información de la Biblioteca Nacional del Perú, declara:

- Que la aceptación de los riesgos es una decisión tomada con entera responsabilidad.
- También entendemos que la aceptación de estos riesgos y sus responsabilidades expirará en un año a partir de la fecha de firma de este documento.
- Los riesgos identificados han sido revisados y aprobados por los integrantes del Comité de Gestión de Seguridad de la Información.
- La aceptación actual de este riesgo no significa que con un cambio de las condiciones actuales en que se encuentre estos riesgos pueden ser mitigados en un futuro con las condiciones financieras técnicas y administrativas adecuadas.
- Hemos leído la declaración y estamos de acuerdo en aceptar los siguientes riesgos:

N°	Código	Nombre de Riesgo	Nivel de Riesgo
1			
2			
3			
4			
5			
Proceso:			
Fecha:			

BIBLIOTECA NACIONAL DEL PERÚ — Oficial de Seguridad de la Información

Nombre y firma del Propietario del Riesgo

Nombre y firma del Presidente del CGSI

Anexo 04: Formato Declaración de Aplicabilidad

biblioteca nacional del perú	Formato	Código	SGSI-FO-12
	Declaración de Aplicabilidad	Versión	01
		Página	

Cláusula N°	Objetivos de Control	Control	Aplica SI/NO	Justificación de la Exclusión o Inclusión	Documento relacionado

Anexo 05: Tabla de Amenazas

Nro.	Tipo	Amenaza
01	Daño físico	Incendio
02		Daño por agua
03		Contaminación
04		Accidente mayor
05		Destrucción del equipo o los medios
06		Polvo, corrosión, congelación
07	Eventos naturales	Fenómeno climático
08		Fenómeno sísmico
09		Inundación
10	Pérdida de servicios esenciales	Fallas del sistema de aire acondicionado o del suministro de agua
11		Pérdida del suministro de electricidad
12		Falla del equipo de telecomunicaciones
13	Compromiso de la información	Introducción de falsa información
14		Fuga de información
15		Alteración de la información
16		Corrupción de la información
17		Destrucción de la información
18		Espionaje remoto
19		Interceptación de comunicaciones
20		Robo de medios o documentos o información
21		Robo de equipos
22		Hallazgo de medios reciclados o descartados
23		Divulgación
24		Datos de fuentes no confiables

BIBLIOTECA NACIONAL DEL PERU – Oficial de Seguridad de la Información

Nro.	Tipo	Amenaza
25		Adulteración del Hardware
26		Adulteración del software
27	**Fallas técnicas**	Falla de equipo
28		Mal funcionamiento del equipo
29		Saturación del sistema de información
30		Mal funcionamiento del software
31	**Acciones no autorizadas**	Uso no autorizado del equipo
32		Copia fraudulenta del software
33		Uso de software falsificado o copiado
34		Errores de mantenimiento /actualización de programas (software)
35		Errores de mantenimiento /actualización de equipos (hardware)
36		Procesamiento ilegal de datos
37	**Compromiso de funciones**	Error en el uso
38		Errores de los usuarios
39		Errores del administrador
40		Errores de configuración
41		Abuso de derechos
42		Falsificación de derechos
43		Negación de acciones
44		Ruptura en la disponibilidad del personal
45	**Criminal informático**	Crimen informático (acoso cibernético)
46		Acto fraudulento (reproducción de archivos, suplantación, intercepción)
47		Soborno informático
48		Ataque al sistema (ej. DDOS)
49		Penetración en el sistema
50		Adulteración del sistema
51		Ingeniería social
52		Acceso no autorizado al sistema
53	**Personal de la entidad (Personal mal capacitado, negligencia, etc.)**	Huelga
54		Chantaje
55		Búsqueda de información propietaria
56		Abuso informático
57		Fraude y robo
58		Soborno por información
59		Ingreso de datos falsificados o corruptos
60		Códigos maliciosos (ej. Virus, bomba lógica, troyano)

BIBLIOTECA NACIONAL DEL PERU
Oficial de Seguridad de la Información

Nro.	Tipo	Amenaza
61		Venta de información personal
62		Intrusión en el sistema
63		Sabotaje al sistema
64	**Agentes de deterioro en material bibliográfico y documental**	Fuerzas físicas (vibración, compresión, fricción, choque, tensión)
65		Criminosos (hurto, robo o vandalismo)
66		Fuego
67		Agua
68		Plagas
69		Poluyentes (ej.: aerosoles, etc.)
70		Radiación: Luz (radiación visible) y radiación UV (radiación ultravioleta) e IR (radiación infrarroja)
71		Temperatura
72		Humedad
73		Disociación: Pérdida de datos e informaciones referentes a los objetos de la colección. Pérdida de la capacidad de recuperar o asociar objetos y/o informaciones. Perdida de objetos de la colección (dentro de la propia institución).

BIBLIOTECA NACIONAL DEL PERÚ
Oficial de Seguridad de la Información

Anexo 06: Tabla de Vulnerabilidades

Nro.	Categoría	Vulnerabilidad
01	**Hardware**	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento
02		Susceptibilidad a la humedad, al polvo y a la suciedad
03		Sensibilidad a la radiación electromagnética
04		Falta de control eficiente del cambio de configuración
05		Susceptibilidad a variación de voltaje
06		Susceptibilidad a variaciones de temperatura
07		Almacenamiento no protegido
08		Falta de cuidado al descartarlo
09	**Software**	Pruebas al software inexistentes o insuficientes
10		Errores conocidos en el software
11		No hacer "logout" cuando se sale de la estación de trabajo
12		Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente
13		Falta de evidencia de auditoria
14		Asignación equivocada de derechos de acceso
15		Software ampliamente distribuido
16		Aplicar programas de aplicación a datos incorrectos en términos del tiempo
17		Interfaz de usuario complicada
18		Falta de documentación
19		Seteo incorrecto de parámetros
20		Fechas incorrectas
21		Falta de mecanismos de identificación y autentificación como la autentificación de usuarios
22		Tablas de claves no protegidas
23		Mala administración de claves
24		Habilitación de servicios innecesarios
25		Software inmaduro o nuevo
26		Especificaciones no claras o incompletas para los desarrolladores
27		Falta de control de cambios eficaz
28		Descarga y uso incontrolado de software
29		Falta de copias de respaldo
30		No producir informes de gestión
31	**Red informática**	Falta de pruebas de envió o recepción de mensaje
32		Líneas de comunicación no protegidas
33		Tráfico delicado no protegido

BIBLIOTECA NACIONAL DEL PERÚ · Oficial de Seguridad de la Información

Nro.	Categoría	Vulnerabilidad
34		Juntas malas en el cableado
35		Punto de falla única
36		Falta de identificación y autentificación de destinado y destinatario
37		Arquitectura de red insegura
38		Transferencia de claves en claro
39		Gestión inadecuada de la red (capacidad de recuperación del ruteo)
40		Conexiones no protegidas de la red publica
41	**Personal de la entidad**	Ausencia del personal
42		Procedimientos inadecuados del reclutamiento
43		Capacitación de seguridad insuficiente
44		Uso incorrecto del software y hardware
45		Falta de conciencia de seguridad
46		Falta de mecanismos de monitoreo
47		Trabajo no supervisado del personal externo o de limpieza
48		Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería
49	**Sitio**	Uso inadecuado o negligente del control de acceso físico a edificios y ambientes
50		Ubicaciones en una área susceptible a las inundaciones
51		Red inestable de energía eléctrica
52		Falta de protección física del edificio, puertas y ventanas
53	**Institución**	Falta de un procedimiento formal para el registro y baja de usuarios
54		Falta de proceso formal para revisar el derecho de acceso (supervisión)
55		Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros
56		Falta de procedimientos de monitoreo de instalaciones de procesamiento de la información
57		Falta de auditorías regulares (supervisión)
58		Falta de procedimientos de identificación y evaluación del riesgo
59		Falta de informes de fallas registradas en los registros del administrador y del operador
60		Respuesta inadecuada del mantenimiento del servicio
61		Falta de procedimiento de control de cambios
62		Falta de procedimiento formal para el control de la documentación de la BNP
63		Falta de proceso formal para autorización de información pública disponible
64		Falta de asignación apropiada de responsabilidades de seguridad en la información

BIBLIOTECA NACIONAL DEL PERÚ · Oficial de Seguridad de la Información

Nro.	Categoría	Vulnerabilidad
65		Falta de planes de continuidad
66		Falta de una política de uso de correos electrónicos
67		Falta de procedimientos para introducir software en sistemas operativos
68		Faltas de registro en los historiales del administrador y del operador
69		Falta de procedimientos para manejo de la información clasificada
70		Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con
71		Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información
72		Falta de política formal sobre el uso de computadoras portátiles
73		Falta de control de activos que se encuentran fuera del local
74		Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"
75		Falta de autorización al acceso a las instalaciones de procesamiento de la información
76		Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad
77		Falta de procedimientos para reportar debilidades en la seguridad
78		Falta de procedimientos sobre el cumplimiento de disposiciones respecto de derechos intelectuales
79		Falta de mantenimiento preventiva en la edificación y equipamientos, la naturaleza de los acervos (materiales
80		Falta de sistemas de detección y supresión automática de incendios
81		Falta de capacitación al personal para responder en caso de un amago incendio