DIRECTORIO

RESOLUCIÓN DE DIRECTORIO N° 037/2025

ASUNTO: **GERENCIA GENERAL – ACTUALIZAR EL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DEL BCB.**

VISTOS:

La Constitución Política del Estado (CPE) de 7 de febrero de 2009.

La Ley N° 1670 de 31 de octubre de 1995 del Banco Central de Bolivia (BCB).

La Ley N° 164 de 8 de agosto de 2011 General de Telecomunicaciones, Tecnologías de Información y Comunicación.

El Decreto Supremo N° 1793 de 13 de noviembre de 2013 que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación.

El Decreto Supremo N° 2514 de 9 de septiembre de 2015 de creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).

El Decreto Supremo N° 3251 de 12 de julio de 2017.

La Resolución Administrativa AGETIC/RA/0051/2017 de 9 de septiembre de 2017 de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).

El Reglamento del Comité de Tecnologías y Seguridad de la Información, aprobado mediante Resolución de Directorio N° 73/2018 de 19 de junio de 2018 y sus modificaciones.

El Estatuto del BCB aprobado mediante Resolución de Directorio N°095/2022 de 6 de octubre de 2022.

La Resolución de Directorio N° 121/2022 de 15 de diciembre de 2022.

//2. R.D. N° 037/2025

El informe BCB-SGR-RSI-INF-2025-13 de 20 de febrero de 2025, emitido por la Subgerencia de Gestión de Riesgos (SGR).

El informe BCB-GAL-SANO-DLBCI-INF-2025-63 de 28 de febrero de 2025, emitido por la Gerencia de Asuntos Legales (GAL).

CONSIDERANDO:

Que la Constitución Política del Estado en el Parágrafo II del Artículo 103 establece que el Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.

Que el Artículo 1 de la Ley N° 1670, establece que el Banco Central de Bolivia, es una institución del Estado, de derecho público, de carácter autárquico, de duración indefinida, con personalidad jurídica y patrimonio propios y con domicilio legal en la ciudad de La Paz. Es la única autoridad monetaria y cambiaria del país, con competencia administrativa, técnica y financiera y facultades normativas especializadas de aplicación general en la forma y con los alcances establecidos en dicha Ley.

Que el Artículo 44 de la referida Ley, señala que la máxima autoridad del BCB es su Directorio, que es responsable de definir sus políticas, normativas especializadas de aplicación general y normas internas; así como establecer estrategias administrativas, operativas y financieras del BCB, aprobando sus respectivos programas de corto y mediano plazo.

Que el inciso a) del Artículo 54 de la Ley N° 1670, establece que el Directorio del BCB tiene la atribución de dictar las normas y adoptar las decisiones generales que fueran necesarias para que el BCB cumpla las funciones, competencias y facultades que le asigna la Ley.

Que el Parágrafo I del Artículo 72 de la Ley N° 164, determina que el Estado en todos sus niveles, fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, el despliegue y uso de infraestructura, el desarrollo de contenidos y

aplicaciones, la protección de las usuarias y usuarios, la seguridad informática y redes, como mecanismos de democratización de oportunidades para todos los sectores de la sociedad y especialmente para aquellos con menores ingresos y con necesidades especiales.

Que el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, aprobado por Decreto Supremo N° 1793, en su inciso b), Parágrafo VI del Artículo 3, define a la seguridad de la información, como la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucrados otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

Que el Decreto Supremo N° 2514, en su Artículo 17, Parágrafo III, establece que las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el Centro de Gestión de Incidentes Informáticos (CGII).

Que los incisos f) e i) del Artículo 7 del citado Decreto Supremo, disponen que la AGETIC tiene la función de establecer los lineamientos técnicos en seguridad de información para las entidades del sector público y elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática.

Que los Lineamientos para la Elaboración e Implementación de los planes institucionales de seguridad de la información de las entidades del sector público tienen como objetivo establecer los lineamientos para que las entidades del sector público del Estado Plurinacional de Bolivia puedan elaborar e implementar sus Planes Institucionales de Seguridad de la Información, en concordancia con la normativa vigente.

Que en el marco de lo dispuesto en el Parágrafo III de la Disposición Transitoria Primera del Decreto Supremo N° 3251, los Planes Institucionales establecidos en dicho Decreto Supremo, podrán ser modificados por cada entidad pública y aprobadas en los casos que corresponda, mediante Resolución expresa.

//4. R.D. N° 037/2025

Que los incisos d) y f) del Artículo 5 del Reglamento del Comité de Tecnologías y Seguridad de la Información del BCB aprobado por Resolución de Directorio N° 073/2018, que establece que el Comité es el único órgano facultado para proponer al Directorio del BCB la aprobación de políticas y lineamientos referidos a las TIC y Seguridad de la Información, así como para revisar el Plan Institucional de Seguridad de la Información (PISI) y promover su aprobación a través del Directorio del BCB.

Que el informe BCB-SGR-RSI-INF-2025-13 de la SGR, concluye que los ajustes propuestos para la actualización del Plan Institucional de Seguridad de la Información del BCB Versión 3, son viables técnicamente y necesarios para dar cumplimiento con los lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público de la AGETIC, el Plan Estratégico Institucional del Banco Central de Bolivia y los nuevos escenarios y riesgos en el contexto dinámico del BCB y las TIC, identificados mediante la Metodología de Gestión de Riesgos de Seguridad de la Información establecida. Asimismo, recomienda al Directorio del BCB la aprobación del Plan Institucional de Seguridad de la Información en su Versión 3.

Que el informe BCB-GAL-SANO-DLBCI-2025-63 de 28 de febrero de 2025 de la GAL, concluye de acuerdo a la justificación expuesta por la SGR en el informe BCB-SGR-RSI-INF-2025-13, para la actualización del PISI-BCB Versión 3, la misma no contraviene el ordenamiento jurídico, por lo que, es legalmente procedente, recomendando al Directorio del BCB su aprobación. Asimismo corresponde dejar sin efecto la Resolución de Directorio N° 121/2022 de 15 de diciembre de 2022 con la que se aprobó el PISI Versión 2.

POR TANTO,
EL DIRECTORIO DEL BANCO CENTRAL DE BOLIVIA
RESUELVE:

Artículo 1.- Aprobar la actualización del Plan Institucional de Seguridad de la Información del Banco Central de Bolivia (PISI-BCB) Versión 3 que en Anexo forma parte de la presente Resolución.

//5. R.D. N° 037/2025

Artículo 2.- Dejar sin efecto la Resolución de Directorio N° 121/2022 de 15 de diciembre de 2022 con la que se aprobó el Plan Institucional de Seguridad de la Información Versión 2.

Artículo 3.- La Presidencia y la Gerencia General quedan encargadas de la ejecución y cumplimiento de la presente Resolución.

La Paz, 11 de marzo de 2025

FDO. ROGER EDWIN ROJAS ULO, Gumersindo Héctor Pino Guzmán, Miguel Angel Marañon Urquidi, Victor Gonzalo Calisaya Gomez.

//6. R.D. N° 037/2025

BICENTENARIO DE BOLIVIA | BANCO CENTRAL DE BOLIVIA | ESTADO PLURINACIONAL DE BOLIVIA

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI-BCB)

Banco Central de Bolivia

VERSIÓN 3.0 GESTIÓN 2025	ELABORADO POR: *Responsable de Seguridad de la Información (RSI)*
	APROBADO POR: *Directorio del Banco Central de Bolivia*

Vo.Bo. BCB

Vo.Bo. BCB

NB/ISO 9001 IBNORCA

ÍNDICE GENERAL

//8. R.D. N° 037/2025

CAPÍTULO 1
ANTECEDENTES

1. ANTECEDENTES

1.1. Funciones del BCB

El Banco Central de Bolivia (BCB) es una institución de derecho público, de carácter autárquico, de duración indefinida, con personalidad jurídica y patrimonio propios. En el marco de la política económica del Estado, el objeto del BCB es procurar la estabilidad del poder adquisitivo interno de la moneda nacional, para contribuir al desarrollo económico y social.

Son atribuciones del BCB, en coordinación con la política económica determinada por el Órgano Ejecutivo, además de las señaladas por la ley, las siguientes:

1.1.1. Determinar y ejecutar la política monetaria

Al tener la responsabilidad de determinar y ejecutar la política monetaria, el BCB controla y regula la cantidad de dinero circulante en la economía del país.

El BCB regula el volumen de crédito interno de acuerdo con su programa monetario. Al efecto, emite, coloca o adquiere títulos valores (letras, bonos, pagarés y otros) y realiza otras operaciones de mercado abierto. Además, tiene la facultad para establecer encajes legales de obligatorio cumplimiento por las entidades de intermediación financiera. Los encajes legales son porcentajes de los depósitos totales que las entidades del sistema financiero deben mantener en el BCB como reserva obligatoria.

El encaje y los depósitos constituidos en el BCB por las entidades de intermediación financiera no están sujetos a ningún tipo de embargo o retención judicial por terceros.

1.1.2. Ejecutar la política cambiaria

El BCB ejecuta la política cambiaria normando la conversión del boliviano con relación a las monedas de otros países. Esta política se orienta a mitigar las presiones inflacionarias de origen externo y preservar la estabilidad del sistema financiero.

Está facultado para normar las operaciones financieras con el extranjero, realizadas por personas o entidades públicas y privadas.

El BCB lleva el registro de la deuda externa pública y privada.

1.1.3. Regular el sistema de pagos

El BCB regula el sistema de pagos, destinado a promover la seguridad y eficiencia de las transacciones.

El sistema de pagos es un conjunto de instrumentos, procedimientos y normas para la transferencia de fondos entre personas naturales y/o jurídicas, que se efectúa utilizando desde dinero en efectivo, cheques, títulos valores, tarjetas de pago hasta dinero electrónico.

1.1.4. Autorizar la emisión de la moneda

El BCB ejerce en forma exclusiva e indelegable la función de emitir la unidad monetaria de Bolivia, "el Boliviano", en forma de billetes y monedas metálicas. En la actualidad ejerce esta función contratando la impresión de billetes y la acuñación de monedas, incluidas las que se emitan con fines conmemorativos o numismáticos.

Los billetes y monedas que emite son medios de pago de curso legal en todo el territorio nacional, con poder liberatorio ilimitado. Los billetes deben llevar las firmas del Presidente y del Gerente General del BCB y el número de serie.

1.1.5. Administrar las reservas internacionales

El BCB tiene la atribución de administrar las reservas internacionales, las cuales se consideran inembargables y no pueden ser objeto de medidas precautorias, administrativas ni judiciales.

Las reservas internacionales están constituidas principalmente por:

- Oro físico.
- Divisas depositadas en el propio BCB o en instituciones financieras fuera del país a la orden del Ente Emisor.
- Letras de cambio y pagarés en favor del BCB.
- Títulos públicos y otros títulos negociables emitidos por gobiernos extranjeros, entidades y organismos internacionales o instituciones financieras de primer orden del exterior.
- Aportes propios a organismos financieros internacionales.

1.2. Misión

"Mantener la estabilidad del poder adquisitivo interno de la moneda nacional, para contribuir al desarrollo económico y social."

1.3. Visión

"El BCB es una entidad líder, reconocida por su credibilidad, transparencia y confianza de la población, que presta servicios con calidad, con tecnologías de información innovadoras, con personal de excelencia y comprometido con los valores institucionales, para el cumplimiento de su misión en el marco del desarrollo integral para el vivir bien."

1.4. Plan Estratégico Institucional (PEI) del BCB

El Plan Institucional de Seguridad de la Información (PISI) del BCB se basa en los objetivos estratégicos del Plan Estratégico Institucional (PEI) 2021-2025, aprobado mediante Resolución Ministerial N° 193 de 11 de julio de 2022 por el Ministerio de Economía y Finanzas Públicas.

El BCB ha establecido los siguientes Objetivos Estratégicos y Estrategias para el periodo 2021-2025:

Objetivo Estratégico 1.-

Mantener la eficiencia y efectividad de las políticas del BCB para preservar la estabilidad del poder adquisitivo interno de la moneda nacional para contribuir al desarrollo económico y social del país, y suscribir anualmente el acuerdo del programa fiscal financiero, permitiendo la ejecución de la política monetaria, la política cambiaria, la regulación del sistema de pagos, la autorización de la emisión de la moneda y la administración de las reservas internacionales.

Estrategia 1.1. *Elaborar y suscribir el Acuerdo del Programa Fiscal y Financiero en forma coordinada con el Órgano Ejecutivo.*

Estrategia 1.2. *Desarrollar e implementar propuestas para perfeccionar la efectividad de la política monetaria, con el fin de controlar la inflación y apoyar el dinamismo de la actividad económica.*

Estrategia 1.3. *Ejecutar una política cambiaria consistente con los objetivos de la política monetaria.*

Estrategia 1.4. *Promover, realizar y difundir, estadísticas, indicadores, investigaciones, análisis encuestas y/o acciones para la generación del conocimiento y propuestas relacionadas en materia económica.*

Estrategia 1.5. *Administrar las Reservas Internacionales bajo criterios de seguridad, preservación de capital, liquidez, diversificación y rentabilidad, que permitan atender las obligaciones de pagos internacionales y los requerimientos de liquidez del sistema financiero.*

Estrategia 1.6. *Cumplir oportunamente con los compromisos del país con relación a la deuda externa pública, así como requerimientos de operaciones cambiarias y de comercio exterior.*

Estrategia 1.7. *Ejecutar las operaciones de mercado abierto con el sistema financiero y otras autorizadas por el Directorio, en base a los lineamientos de la política monetaria, establecidos.*

Estrategia 1.8. *Ejecutar oportunamente las operaciones monetarias del BCB con el sector público, así como personas naturales y jurídicas del sector privado.*

Estrategia 1.9. *Garantizar la provisión del material monetario a las entidades financieras.*

Estrategia 1.10. *Promover la modernización, eficiencia y seguridad del sistema de pagos nacional a través de la regulación, vigilancia y la administración del sistema de pagos electrónico del BCB.*

Estrategia 1.11. *Gestionar las operaciones de créditos y préstamos de liquidez del sistema financiero para prevenir riesgos.*

Estrategia 1.12. *Contribuir a la preservación de la estabilidad financiera mediante el análisis de los riesgos del sistema financiero y la formulación de políticas de carácter macroprudencial.*

Estrategia 1.13. *Administrar las acreencias y formular políticas para optimizar la recuperación de la cartera y disposición de los bienes realizables, recibidos en dación en pago, a título gratuito, en administración y adjudicados.*

Estrategia 1.14. *Fortalecer y contribuir a la continuidad y la modernización de las operaciones que desarrolla el BCB a través de los proyectos de infraestructura y la implementación de nuevas tecnologías de información y comunicación.*

Objetivo Estratégico 2.-

Promover y mantener la bolivianización financiera a través de la innovación de medidas e incentivos.

Estrategia 2.1. *Desarrollar y proponer políticas que mantengan y consoliden la bolivianización financiera de la economía.*

Vo.Bo. BCB

Vo.Bo. BCB

NB/ISO 9001 IBNORCA

Objetivo Estratégico 3.-

Mantener una gestión eficiente e inclusiva para una administración institucional apropiada, utilizando adecuadamente los recursos y la planificación como herramienta de gestión institucional.

***Estrategia 3.1.** Fortalecer la gestión institucional bajo criterios de calidad, oportunidad y eficiencia.*

Objetivo Estratégico 4.-

Promover y consolidar una gestión pública transparente a través de la Rendición Pública de Cuentas y la participación efectiva de la sociedad civil e institucionalización del Control Social, así como la evaluación periódica del Control Interno.

***Estrategia 4.1.** Promover y fortalecer las medidas y acciones que permitan prevenir posibles hechos de corrupción, así como aquellas acciones orientadas a mejorar la participación ciudadana y la rendición pública de cuentas.*

***Estrategia 4.2.** Fortalecer el control interno del BCB a través de evaluaciones y recomendaciones de auditoria.*

CAPÍTULO 2
ETAPA INICIAL

2. ETAPA INCIAL DEL PLAN

2.1. FUENTES PRINCIPALES PARA LA ELABORACIÓN DEL PISI

Las fuentes principales de insumo para el presente Plan, son:

2.1.1. Flujo de información del BCB en el marco de la Ley 1670.

El Banco Central de Bolivia cumple sus funciones en el marco de la Ley 1670 y se relaciona con los siguientes tipos de entidades, no limitativo, para el flujo de información que apoya sus operaciones:

- Ministerio de Economía y Finanzas Públicas (MEFP).
- Entidades del Sector Público.
- Autoridad de Supervisión del Sistema Financiero (ASFI).
- Entidades del Sistema Financiero.
- Instituciones Financieras Internacionales.

2.1.2. Normativa Interna

El Banco Central de Bolivia para el cumplimiento de sus funciones y desarrollar sus operaciones ha establecido la siguiente normativa interna:

- Estatuto del Banco Central de Bolivia.
- Plan Estratégico Institucional (PEI 2021-2025).
- Manual de Procesos del Banco Central de Bolivia.
- Manual de Organización y Funciones del BCB.
- Plan Operativo Anual de la Gestión 2024 y 2025.
- Reglamento de Seguridad de la Información.
- Reglamento de Gestión de Riesgo y Continuidad de Negocio.
- Reglamento de Gestión Documental del BCB.
- Reglamento Interno de Personal del BCB.
- Procedimientos y Guías operativas de Gestión del Inventario y Clasificación de Activos de Información.
- Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Procedimiento Actualización de Datos Personales de los Servidores Públicos del BCB, en relación al "Compromiso de Confidencialidad y Uso Adecuado de los Servicios y Recursos del BCB".

2.1.3. Evaluaciones de riesgos efectuados y gestión de incidentes

El Banco Central de Bolivia efectúa la gestión de riesgos operativos, de seguridad de la información y gestión de incidentes, mediante las siguientes acciones:

- Las áreas organizacionales del BCB, en coordinación con la Subgerencia de Gestión de Riesgos implementan la gestión de riesgo operativo de manera sistemática y estructurada a través de: la identificación de riesgos. mecanismos de control y la definición de la estrategia de tratamiento del riesgo.
- Se ha efectuado evaluaciones de riesgos de seguridad de la información en los Planes Institucionales de Seguridad de la Información históricos:
  - Plan Institucional de Seguridad de la Información, versión 1 de la gestión 2018 (aprobado mediante Resolución de Directorio N° 136/2018).
  - Plan Institucional de Seguridad de la Información, versión 2 de la gestión 2022 (aprobado mediante Resolución de Directorio N° 121/2022).
- Se cuenta con procedimientos y guías para la gestión de incidentes de seguridad de la información, que toman en cuenta la identificación, el análisis, respuesta y recuperación.
- Se cuenta con el inventario de Activos de Información actualizado en abril/2024 en cumplimiento del Reglamento de Seguridad de la Información y octubre/2024, para

la actualización de Responsables y/o Custodios y Sistemas de Información Tecnológicos, actividades que son realizadas en la medida y necesidades del RSI ante cambios sustanciales que se presenten dentro la institución u otros.

2.2. RESPONSABILIDADES Y ROLES

2.2.1. Responsabilidades de la Máxima Autoridad Ejecutiva (MAE) respecto a la seguridad de la información

El Presidente como MAE del BCB, en el marco de sus atribuciones, a través de su Directorio, la Gerencia General e instancias competentes:

- Se encuentra informado a través de los Informes Trimestrales programados en el Calendario Anual de Directorio, elaborados por el Responsable de Seguridad de la Información (RSI), presentado previamente al Gerente General (GGRAL) en coordinación con la Subgerencia de Gestión de Riesgos (SGR), el cual es expuesto en Directorio precedido por el Presidente del BCB.
- A través del RSI, trimestralmente o a requerimiento, toma conocimiento de la normativa vigente respecto a seguridad de la información, establecido en el Decreto Supremo N° 2514 de 9 de septiembre de 2015, Decreto Supremo N° 1793, de 13 de noviembre de 2013, de reglamentación a la Ley 164 y demás normativa aplicable. Asimismo, informa sobre el cumplimiento del Reglamento de Seguridad de la Información del Banco Central de Bolivia (BCB), aprobado mediante Resolución de Directorio N°122/2023 de 5 de septiembre de 2023.
- Designó al Responsable de Seguridad de la Información (RSI), comunicada a la AGETIC a través de nota BCB-SGR-RSI-CE-2023-1 de 27 de marzo de 2023.
- Conforma el Comité de Tecnología y Seguridad de la Información (CTSI) aprobado mediante Resolución de Directorio N°073/2018 de 19 de junio de 2018.
- Aprueba el Plan Institucional de Seguridad de la Información (PISI), a través del Directorio, mediante Resolución de Directorio que resuelve su ejecución y cumplimiento por las instancias competentes del BCB.

2.2.2. Designación y Funciones del Responsable de Seguridad de la Información

El RSI, cuenta con las siguientes funciones generales:

a) Elaborar y proponer el Plan Institucional de Seguridad de la Información del BCB.
b) Elaborar y proponer las Políticas en relación a la seguridad de la información del BCB.
c) Elaborar manuales de procesos y/o procedimientos de seguridad específicos que se desprendan de los lineamientos del PISI y promover su aprobación y difusión en el BCB.

d) Elaborar y/o actualizar e reglamento que apoye la gestión de seguridad de la información del BCB.
e) Evaluar riesgos, amenazas y vulnerabilidades y proponer medidas preventivas y correctivas en materia de seguridad de la información.
f) Gestionar y coordinar la atención y respuesta a incidentes de seguridad de la información del BCB.
g) Coordinar con la Gerencia de Sistemas la implementación de controles, métodos y sistemas de seguridad, que permitan controlar la confidencialidad, integridad y disponibilidad de la información en los sistemas informáticos y servicios TI en general.
h) Implantar programas de inducción, capacitación, comunicación y sensibilidad de seguridad de la información para el recurso humano del BCB.
i) Planear proyectos y actividades orientadas a la mejora de la seguridad de la información e implementar los aprobados.
j) Proponer evaluaciones externas del nivel de seguridad de la información en el que se encuentre el BCB.
k) Coordinar la realización, actualización, valoración y clasificación del inventario de Activos de Información del BCB.
l) Informar y asesorar de manera oportuna a la Alta Dirección, sobre los riesgos de seguridad de la información de la entidad, a fin de coadyuvar en la óptima toma de decisiones.
m) Otras de su competencia que le sean encomendadas por sus superiores jerárquicos.

2.2.3. Conformación y funciones del Comité de Tecnología y Seguridad de la Información (CTSI)

La conformación y funciones del CTSI, se encuentran establecidas en el Reglamento del Comité de Tecnología y Seguridad de la Información aprobado a través de Resolución de Directorio N° 073/2018 de 19 de junio de 2018 del BCB.

El CTSI está conformado por los siguientes miembros:

a) El Presidente del BCB.
b) El Gerente General del BCB.
c) Un Gerente de un área sustantiva designado por el Gerente General.
d) Un Gerente de un área de apoyo designado por el Gerente General.
e) El Gerente de Sistemas.
f) Un Subgerente de la Gerencia de Sistemas designado por el Gerente de Sistemas.
g) El Responsable de Seguridad de la Información (RSI), cuando se traten temas de Seguridad de la Información.

El CTSI asume como mínimo las siguientes funciones o facultades:

a) Revisar el Plan Institucional de Seguridad de la Información (PISI) y promover su aprobación a través del Directorio del BCB.
b) Revisar los manuales de procesos y/o procedimientos de seguridad que se desprendan de la Política de Seguridad de la Información incorporada en el PISI.
c) Proponer estrategias necesarias para la implementación y/o fortalecimiento de controles de seguridad en el marco de la mejora continua.
d) Realizar el seguimiento y control de los indicadores y métricas establecidos y definir las acciones que correspondan al respecto.
e) Proponer y promover las acciones necesarias en función a la gravedad de los incidentes de seguridad de la información, con el fin de prevenir incidentes futuros.

CAPÍTULO 3
EVALUACIÓN DE CONTROLES

3. EVALUACIÓN DE CONTROLES IMPLEMENTADOS

A continuación, se detalla el cumplimiento de las actividades para controlar los riesgos identificados y la evaluación de los controles implementados e indicadores establecidos.

1 – PROTECCIÓN ANTE TRANSACCIONES FRAUDULENTAS		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Riesgo A.1.4.: Compromiso de certificados digitales y llaves privadas asociadas a operaciones críticas. **Nivel de Riesgo**: Alto **Control**: 7.3.1 Transferencia de información **Actividad:** Implementar herramientas especializadas para el resguardo y uso de los certificados digitales y llaves privadas.	GSIS	Dic/23 **IMPLEMENTADO** Se implementó Bóveda de contraseñas para usuarios privilegiados (usuario "root") **Evaluación**. El control 7.3.1. Transferencia de información y su especificidad de acuerdo a los Lineamientos del PISI es adecuado para preservar la integridad de la información transferida o de las operaciones a través de proteger el acceso no autorizado de certificados digitales y llaves privadas asociadas a operaciones. **Indicador. IM-A.1.4.** *Cantidad de certificados digitales y llaves privadas comprometidas*: Ningún certificado digital o llave privada fue comprometida, por lo cual la evaluación del control implementado fue adecuada.
Riesgo A.1.9.: Actividad anómala o sospechosa en operaciones de sistemas de terceros no detectada. **Nivel de Riesgo**: Medio **Control**: 3.2.1 Administración de accesos, cancelación y privilegios de usuarios **Actividad**: Asegurar que el acceso a los sistemas de terceros sea realizado desde ambientes seguros.	GSIS/GOI/ RSI	Dic/23 **IMPLEMENTADO** Los sistemas SWIFT, Abacus y SIGADE cuentan con accesos seguros. **Evaluación**. El control 3.2.1. Administración de accesos, cancelación y privilegios de usuarios y su especificidad de acuerdo a los Lineamientos del PISI es adecuado para controlar el acceso no autorizado a sistemas provistos por terceros desde las estaciones de trabajo de la Gerencia de Operaciones Internacionales. **Indicador. IM-A.1.9.** *Conexión de sistemas de terceros solo desde ambientes seguros*: Los accesos a los sistemas de terceros se realiza desde ambientes del BCB, los cuales están

1 – PROTECCIÓN ANTE TRANSACCIONES FRAUDULENTAS		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
		controlados y protegidos mediante la actividades y tareas efectuadas, por lo cual el control es adecuado.
Riesgo A.1.10: Actividad anómala o sospechosa en operaciones en sistemas de terceros no detectada. **Nivel de Riesgo**: Medio **Control**: 6.1.2 Gestión de cambios **Actividad**: Gestionar los eventos (logs) de sistemas de terceros.	RSI/GSIS/ Áreas	Dic/24 **IMPLEMENTADO** Los sistemas SWIFT, Abacus y SIGADE cuentan con una gestión de logs a través de herramientas implementadas. **Evaluación**. El control 6.1.2. Gestión de cambios y su especificidad de acuerdo a los Lineamientos del PISI es adecuado para gestionar los eventos que se suscitan en los sistemas provistos por terceros en la Gerencia de Operaciones Internacionales. **Indicador. IM-A.1.10**. *Los Logs de los sistemas de terceros son gestionados*: Se realiza la gestión de logs que abarca gran parte de los sistemas provistos por terceros, por lo cual el control es adecuado.
Riesgo A.1.11. Sistemas de terceros desactualizados. **Nivel de Riesgo**: Alto **Control**: 8.2.1 Requisitos de seguridad **Actividad**: Actualización periódica de los sistemas de externos de forma automática o manual.	RSI/GSIS/ Áreas	Dic/23 **IMPLEMENTADO** (Recurrente) El sistema SWIFT, Abacus y SIGADE cuentan con soporte para actualizaciones y se encuentran actualizados. **Evaluación**. El control 8.2.1. Requisitos de Seguridad y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación para la actualización periódica de los sistemas provistos por terceros. **Indicador. IM-A.1.11**. *Sistemas de terceros actualizados periódicamente*: Todos los sistemas de terceros se encuentran actualizados, por lo cual el control es adecuado.
Riesgo A.1.12.: Acceso no autorizado en las comunicaciones con los sistemas de terceros. **Nivel de Riesgo**: Alto **Control**: 8.2.1 Requisitos de seguridad **Actividad**: Implementar firma digital y/o cifrado de datos, en la comunicaciones y transferencia de información desde/hasta los sistemas de terceros.	RSI/GSIS/ Áreas	Dic/24 **IMPLEMENTADO** Los mensajes transmitidos a los sistemas SWIFT, Abacus y SIGADE se encuentran asegurados y protegidos. **Evaluación**. El control 8.2.1. Requisitos de Seguridad y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación para asegurar las comunicaciones y la transferencia de información, particularmente en el sistema SWIFT. **Indicador. IM-A.1.12**. *Sistemas de terceros tienen comunicación segura con sistemas back office*: Los sistemas de terceros se comunican mediante la red local, misma que está controlado y protegido con las acciones realizadas y los controles per se del BCB, por lo cual el control es adecuado.

2 - CONTINUIDAD DE OPERACIONES Y TECNOLOGÍA DE INFORMACIÓN		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Riesgo A.2.2.: Existe información consolidada que está almacenada solamente en las computadoras del personal, mismas que pueden ser pérdidas en caso de algún incidente informático. **Nivel de Riesgo**: Alto **Control**: 6.2.1 Respaldos de información **Actividad**: Almacenar mensualmente y de manera consolida en el Servidor de Archivos del BCB (File Server)	Áreas Sustantivas	Dic/23 **IMPLEMENTADO** Se ha implementado en las áreas el servicio de servidores de archivos mismos que respaldan la información en forma centralizada gestionada la GSIS. Asimismo, se ha implementado el mecanismo de respaldo de información de equipos de usuario de acuerdo a Circular CIG N° 14/2022. **Evaluación**. El control 6.2.1. Respaldos de información y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación para respaldar la información que se encuentra almacenada en los computadores de usuarios.

2 - CONTINUIDAD DE OPERACIONES Y TECNOLOGÍA DE INFORMACIÓN		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Información Sustantiva de las áreas (cuyas fuentes son archivos PDF, Excel, Word, Power Point, entre otros), permitiendo un respaldo a la información que se generan, procesan, transmiten y almacenan de manera local, en las diferentes computadoras del personal.		**Indicador. IM-A.2.2** *Diferencias de información consolidada*: Indicador no está planteado correctamente. Sin embargo, no se ha registrado pérdida de información almacenada en los servidores de archivo.
Riesgo A.2.5.: Interrupción en servicios y/o sistemas informáticos en el BCB. **Nivel de Riesgo:** Alto **Control:** 9.1.1 Gestión de incidentes **Actividad:** Implementar la Gestión de Incidentes de Seguridad de la Información, acorde a normativa vigente.	RSI (Equipo de respuesta ante incidentes) Áreas	Dic/23 **IMPLEMENTADO** Se cuenta con procedimientos y mecanismos para gestionar incidentes de seguridad de la información. Circular CIG N° 07/2023. **Evaluación**. El control 9.1.1. Gestión de Incidentes y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación para la implementación y operativización del proceso de gestión de incidentes de seguridad de la información. **Indicador. IM-A.2.5** *Tiempo de respuesta inicial*: Indicador no está planteado correctamente. Sin embargo, se ha gestionado los incidentes ocurridos en el período.
Riesgo A.2.6.: Interrupción en servicios y/o sistemas informáticos en el BCB **Nivel de Riesgo:** Medio **Control:** 10.1. Implementación del plan de contingencias tecnológicas. **Actividad:** Elaborar, formalizar, actualizar e implementar el plan de contingencias tecnológicas del BCB que incluya sistemas provistos por terceros.	RSI/GSIS/ Áreas	Dic/23 **IMPLEMENTADO** Se cuenta con el Plan de Continuidad de TIC en su versión 3, elaborado por la GSIS. **Evaluación**. El control 10.1. Implementación del plan de contingencias tecnológicas y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación para la elaboración, actualización y ejercicio de un plan de contingencias. **Indicador. IM-A.2.6.** *Se cuenta con un plan de contingencias tecnológicas del BCB implementado que incluye sistemas provistos por terceros*: Se cuenta con el Plan de continuidad de TIC elaborado por la GSIS.

3 –ROBO, PÉRDIDA O FUGA DE INFORMACIÓN		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Riesgo A.3.1.: Existe mucha información generada en las áreas sustantivas que pueden ser extraviadas debido a que el personal desconoce la forma de hacer gestión documental. **Nivel de Riesgo**: Crítico **Control**: 2.1.2 Responsabilidad y custodia de los activos de información **Control:** 2.2.3 Protección del Archivo **Actividad**: Diseñar una guía para el personal del BCB en la cual se expresa la forma adecuada de la manipulación de información existente en las distintas áreas.	Subgerencia de Gestión Documental	Dic/23 **IMPLEMENTADO** Se tiene el Reglamento de Gestión Documental RD N° 42/2023 y procedimientos de la SGDB. **Evaluación**. Los controles 2.1.2 Responsabilidad y custodia de los activos de información y 2.2.3. Protección del Archivo sus especificidades de acuerdo a los Lineamientos del PISI son adecuados como acción de mitigación para el adecuado manejo de los documento y archivos físicos instruidos por el SGDB. **Indicador. IM-A.3.1.** *Existencia de Guía de Gestión documental*: Se cuenta con el Reglamento de Gestión Documental.
Riesgo A.3.2.: Existe mucha información física que puede extraviarse o deteriorarse, misma que por la cantidad	Áreas sustantivas	Dic/23 **IMPLEMENTADO** (Recurrente)

3 –ROBO, PÉRDIDA O FUGA DE INFORMACIÓN		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
de documentos ya no es práctico disponer su almacenamiento físico. **Nivel de Riesgo**: Crítico **Control**: 2.1.2 Responsabilidad y custodia de los activos de información **Control**: 2.2.3 Protección del Archivo **Actividad**: Digitalizar la documentación física que no cuenta con un respaldo de procesamiento de un sistema informático, en las distintas áreas sustantivas.	GADM	El proceso de digitalización de documentos de las áreas es una tarea recurrente gestionado por la SGDB. **Evaluación**. Los controles 2.1.2 Responsabilidad y custodia de los activos de información y 2.2.3. Protección del Archivo sus especificidades de acuerdo a los Lineamientos del PISI son adecuados como acción de mitigación para la gestión y digitalización de información de los documento y archivos físicos. **Indicador. IM-A.3.2** *Porcentaje de implementación de información digitalizada*: la cantidad de documentos digitalizados sobrepasó lo planificado, es decir, más del 100%.
Riesgo A.3.3.: Perdida o fuga de información sensible **Nivel de Riesgo**: Alto **Control**: 2.2.1 Clasificación **Control**: 2.2.2 Etiquetado y manejo **Actividad**: Implementar y/o actualizar la clasificación de la información acorde a Procedimiento y Guía respectiva	RSI/Áreas	Dic/23 **IMPLEMENTADO** Se cuenta con el Inventario de Activos de Información elaborado por las áreas del BCB en coordinación con el RSI que incluye la valoración y clasificación. **Evaluación**. Los controles 2.2.1 Clasificación y 2.2.2 Etiquetado y manejo y sus especificidades de acuerdo a los Lineamientos del PISI son adecuados como acción de mitigación para pérdida o fuga de información mediante la actualización del inventario que instruyó a las áreas efectuar la clasificación de la información. **Indicador. IM-A.3.3** *Porcentaje de información clasificada*: El inventario de activos de información considera la totalidad de activos clasificados, es decir 100%.
Riesgo A.3.4.: Perdida o fuga de información sensible **Nivel de Riesgo**: Alto **Control**: 2.3.1 Gestión de medios removibles **Actividad**: Implementar una herramienta para gestionar, monitorear y registrar actividades de copia de información clasificada en medios removibles.	RSI/GSIS	Oct/22 – Dic/23 **IMPLEMENTADO** Se implementó la herramienta Data Lost Prevention (DLP), instalado en equipos de usuarios del BCB. **Evaluación**. El control 2.3.1 Gestión de medios removibles y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación para evitar la pérdida o fuga de información a través de la herramienta DLP. **Indicador. IM-A.3.4** *Porcentaje de implementación de reglas de protección de información*: El indicador no está planteado correctamente. Sin embargo, la herramienta cuenta con las reglas implementadas de acuerdo a lo definido con la GSIS.

4 – OPORTUNIDAD E INTEGRIDAD EN LAS OPERACIONES		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Riesgo A.4.2. - Al preparar la presentación y reportes, la posibilidad de un error en el cálculo o al digitar podría ocasionar que la misma no tenga datos correctos. - No existe un mecanismo de detección o registro de errores previo, solamente se detectan los errores cuando pasan a otra etapa. - Mala interpretación de instrucciones, datos, normativa u otros. **Nivel de Riesgo**: Alto	GEF	Dic/23 **IMPLEMENTADO** La Subgerencia de Análisis del Sistema Financiero (SASF) ha elaborado las guías y el reporte de errores. **Evaluación**. El control 2.1.2 Responsabilidad y custodia de los activos de información y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación para evitar errores en reportes del SASF. **Indicador. IM-A.4.2** *Solucionario de problemas a reportes específicos*: El indicador no está planteado correctamente, sin embargo, se cuenta con el reporte de errores frecuentes.

4 – OPORTUNIDAD E INTEGRIDAD EN LAS OPERACIONES		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Control: 2.1.2 Responsabilidad y custodia de los activos de información **Actividad**: Crear un reporte de errores frecuentes con el objeto de ser analizados y minimizados, conformando para ello una guía que evite y subsane dichos errores. Los activos involucrados en la presente actividad son: • Reporte FPAH • Reporte FPA • Reporte de la TRE y de la TAPR • Reportes de Tasas de Interés • Reporte de transferencias al/del Fondo RAL		
Riesgo A.4.3.: Pérdida de documentación por inadecuada manipulación de los usuarios o por situaciones imprevistas. **Nivel de Riesgo**: Alto **Control**: 2.1.2 Responsabilidad y custodia de los activos de información **Actividad**: Emitir una Comunicación interna al personal del área, recomendando la forma correcta de manipulación de la Documentación de Acreencias.	GEF	Dic/23 **IMPLEMENTADO** La Subgerencia de Realización y Recuperación de Activos de la GEF ha emitido los documentos para la gestión del archivo de documentos de acreencias. **Evaluación**: El control 2.1.2 Responsabilidad y custodia de los activos de información y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación para evitar errores en el manejo de documentos de acreencias. **Indicador. IM-A.4.3.** *Emisión de comunicación para la manipulación correcta de Documentación de Acreencias*: La Comunicación de la SRRA interna fue emitido.

5 – PÉRDIDA DE MATERIAL MONETARIO, MONEDAS CONMEMORATIVAS Y VALORES		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Riesgo A.5.1.: Error cometido por los servidores públicos asignados al pago de una operación que permita la salida de dinero en demasía. **Nivel de Riesgo**: Alto **Control**: 2.1.2 Responsabilidad y custodia de los activos de información **Actividad**: Verificar y controlar la cantidad de material monetario a pagar en cada operación con sus respectivos antecedentes.	GTES	Dic/23 **IMPLEMENTADO** La SOMM ha establecido los procedimientos correspondientes. **Evaluación**: El control 2.1.2 Responsabilidad y custodia de los activos de información y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación para evitar errores en las operaciones de tesorería. **Indicador. IM-A.5.1.** *Diferencia de material monetario a pagar*: No se ha registrado salida de dineros en demasía en la GTES.
Riesgo A.5.2.: Sustracción de material monetario, monedas conmemorativas y valores en custodio de manera planificada por los servidores públicos que desarrollan sus funciones en el área. **Nivel de Riesgo**: Alto **Control**: 2.1.2 Responsabilidad y custodia de los activos de información	GTES	Dic/23 **IMPLEMENTADO** La GTES mediante la SOMM ha implementado y ejecutado los procedimientos correspondientes. **Evaluación**: El control 2.1.2 Responsabilidad y custodia de los activos de información y su especificidad de acuerdo a los Lineamientos del PISI es adecuado como acción de mitigación y las tareas ejecutadas para evitar la sustracción de material monetario en Tesorería.

5 – PÉRDIDA DE MATERIAL MONETARIO, MONEDAS CONMEMORATIVAS Y VALORES		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Actividad: En los respectivos almacenes, realizar arqueos sorpresivos para verificar la existencia de: • Material monetario • Monedas conmemorativas • Valores en custodia		**Indicador. IM-A.5.2.** *Diferencias en los arqueos*: No se ha registrado sustracción de material monetario en la GTES.
Riesgo A.5.3.: Sustracción de material monetario planificada por los servidores públicos que desarrollan sus funciones en el área. **Nivel de Riesgo**: Alto **Control**: 5.1.1 Seguridad física en áreas e instalaciones **Actividad**: Cumplir estrictamente con los protocolos de ingreso y salida de personas en los ambientes de tesorería.	GTES	Dic/23 **IMPLEMENTADO** La GTES mediante la SOMM ha implementado y ejecutado los procedimientos correspondientes. **Evaluación**. El control 5.1.1 Seguridad en áreas e instalaciones y las acciones implementadas es adecuado como acción de mitigación para evitar sustracción de material monetario en Tesorería. **Indicador. IM-A.5.3**. *Cumplimiento del protocolo de ingreso y salida de personas a ambientes de Tesorería*: No se ha registrado sustracción de material monetario en la GTES.
Riesgo A.5.4.: Deterioro del material monetario por exposición a factores ambientales (humedad, agua, ruido, contaminación, polvo, suciedad). **Nivel de Riesgo**: Alto **Control**: 5.3.1 Condiciones operativas **Actividad**: Realizar el mantenimiento periódico de cañerías de agua y cárcamo (cada 6 meses), para evitar inundaciones y rebalses en los almacenes de material monetario.	GTES/GADM	Dic/23 **IMPLEMENTADO** La GTES en coordinación con la GADM han elaborado y ejecutado los procedimientos necesarios de mantenimiento. **Evaluación**. El control 5.3.1 Condiciones operativas y su especificidad de acuerdo a los Lineamientos del PISI es adecuado para alertar factores ambientales en Tesorería. **Indicador. IM-A.5.4**. *Número de veces por año que se hizo mantenimiento a las cañerías de agua y cárcamo*: La GADM realizó el mantenimiento de las cañerías de agua y cárcamo al menos una vez.
Riesgo A.5.5.: Deterioro de la maquinaria y/o equipo depositado en valores en custodia por exposición a factores ambientales (humedad, agua, ruido, contaminación, polvo, suciedad) que dañen los valores en custodia. **Nivel de Riesgo**: Alto **Control**: 5.3.1 Condiciones operativas **Actividad**: Elaborar un procedimiento para establecer una verificación periódica del estado de conservación de los valores en custodia depositados en gavetas de Bóveda Central.	GTES	Dic/23 **IMPLEMENTADO** Ya no existe maquinaria y/o equipos depositados como valores en custodia al haber ejecutado las acciones necesarias. **Evaluación**. El control 5.3.1 Condiciones operativas y su especificidad de acuerdo a los Lineamientos del PISI es adecuado para controlar el deterioro de valores en custodia por factores ambientales en Tesorería. **Indicador. IM-A.5.5**. *Cantidad de veces por año que se hizo la verificación del estado de conservación de los valores en custodia*: El indicador no está correctamente planteado, dado que el riesgo ya no existe al no existir equipos en custodia.

6 – GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Riesgo A.6.1.: Elevada cantidad de información que se genera en las áreas del BCB, que implica a la vez un desbordamiento de actividades de control y seguimiento a la implantación de las mismas.	RSI	Dic/23 **IMPLEMENTADO** El RSI forma parte de la SGR y se encuentra visibilizada dentro del Organigrama del BCB. **Evaluación**. El control 11.2.1 Evaluación de cumplimiento del plan institucional de seguridad de la información y su especificidad de acuerdo a los Lineamientos del PISI es

//23. R.D. N° 037/2025

6 – GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Nivel de Riesgo: Alto **Control**: 11.2.1 Evaluación de cumplimiento del plan institucional de seguridad de la información **Actividad**: Crear un área organizacional para la atención de temas de seguridad de la información.		adecuado para contar con una gestión de la seguridad de información del BCB. **Indicador. IM-A.6.1** *Presencia de un área organizacional para atender temas de seguridad de información del BCB*: Se cuenta con un área que gestiona los temas de seguridad de la Información dependiente de la Subgerencia de Gestión de Riesgos.

7 – SEGURIDAD FÍSICA Y DEL ENTORNO		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Riesgo A.7.1.: Perdida de información sensible. **Nivel de Riesgo:** Alto **Control:** 5.1.1 Seguridad física en áreas e instalaciones **Actividad:** Implementar el Sistema de Video Vigilancia en los ambientes de Tesorería.	SGR	Dic/24 **IMPLEMENTADO** Se modernizó y mejoró el sistema de video-vigilancia, dotándole en áreas restringidas de Tesorería la funcionalidad de VIDEOVIGILANCIA CON AUDIO BI-DIRECCIONAL **Evaluación**. El control 5.1.1 Seguridad física en áreas e instalaciones y su especificidad de acuerdo a los Lineamientos del PISI es adecuado para apoyar la seguridad física del área de tesorería. **Indicador. IM-A.7.1** *Porcentaje de implementación del sistema de videovigilancia*: El indicador no está correctamente planteado, es ambiguo y genérico. Sin embargo, se encuentra implementado el sistema de videovigilancia.
Riesgo A.7.2.: Acceso no autorizado a las áreas seguras de Tesorería. **Nivel de Riesgo:** Alto **Control:** 5.1.1 Seguridad física en áreas e instalaciones **Actividad:** Implementar el Sistema de Control de Accesos en los ambientes de Tesorería.	GSIS/SGR	Dic/2024 **IMPLEMENTADO** Se ha Implementado y renovado los sistemas de alarmas de intrusión en Tesorería Se ha Implementado y mejorado el sistema de control de acceso biométrico con integración al Sistema de Video vigilancia, en todas las puertas de ingresos y salidas de los ambientes restringidos de Tesorería. Se tiene un sistema para solicitudes, control y autorizaciones de visitas. **Evaluación**. El control 5.1.1 Seguridad física en áreas e instalaciones y su especificidad de acuerdo a los Lineamientos del PISI es adecuado para contar con una gestión de la seguridad física a través de la implementación de control de acceso con integración al sistema de video vigilancia en Tesorería. **Indicador. IM-A.7.2** *Porcentaje de implementación del sistema de control de accesos*: El indicador no está correctamente planteado, es ambiguo y genérico. Sin embargo, se encuentra implementado el sistema de control de accesos con nuevas funcionalidades.
Riesgo A.7.3.: Probabilidad de desastre por incendio, inundación, averías, corte de suministro eléctrico **Nivel de Riesgo:** Alto **Control:** 5.1.1 Seguridad física en áreas e instalaciones **Actividad:** Implementar el Sistema de Alarmas en los ambientes de Tesorería **Alineación PEI:** Estrategia 1.14	SGR	Dic/24 **IMPLEMENTADO** Se cuenta con un sistema de alarmas y sensores para fortalecer la seguridad de los ambientes de Tesorería. **Evaluación**. El control 5.1.1 Seguridad física en áreas e instalaciones y su especificidad de acuerdo a los Lineamientos del PISI es adecuado para contar con una gestión de la seguridad física a través de la implementación de sistemas de alarmas en Tesorería. **Indicador. IM-A.7.3** *Porcentaje de implementación del sistema de alarmas*: El indicador no está correctamente planteado, es ambiguo y genérico. Sin embargo, se encuentra implementado el sistema de alarmas.

7 – SEGURIDAD FÍSICA Y DEL ENTORNO		
ESCENARIO / RIESGO / CONTROLES / ACTIVIDADES / ALINEACIÓN	**ÁREA EJECUTORA**	**FECHA / CUMPLIMIENTO**
Riesgo A.7.5.: Trabajos no autorizados dentro las áreas seguras. **Nivel de Riesgo:** Alto **Control:** 5.1.2 Trabajo en áreas e instalaciones seguras **Actividad:** Gestionar las actividades de trabajo y operación dentro de las áreas seguras acorde a los requisitos de seguridad.	SGR	Jun/23 **IMPLEMENTADO** Se cuenta con el Reglamento de Seguridad de la información, aprobado mediante RD N° 122/2023. El área de Tesorería cuenta con el "Protocolo de Ingresos y salidas de Personas, Bienes, Vehículos y otros Materiales a los ambientes restringidos de Tesorería del BCB". La GSIS para los CPDs cuenta con procedimientos respectivos. **Evaluación**. El control 5.1.2 Trabajo en áreas e instalaciones y su especificidad de acuerdo a los Lineamientos del PISI es adecuado para gestionar el trabajo en áreas seguras del BCB. **Indicador. IM-A.7.3.** *Trabajos no autorizados dentro de las áreas seguras*: El indicador no está correctamente planteado, es ambiguo y genérico. Sin embargo, se han implementado controles normativos que gobiernan los trabajos dentro de las áreas seguras.

CAPÍTULO 4
DESARROLLO DEL PLAN

4. DESARROLLO

4.1. Introducción

En el marco a lo dispuesto en el Decreto Supremo N° 2514 de 9 de septiembre de 2015 y los "*Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público*", aprobado mediante Resolución Administrativa AGETIC /RA/0051/2017 de 19 de septiembre de 2017, que definen las directrices técnicas para establecer una mejora continua del nivel de madurez de los controles de seguridad de la información que están aplicados en el Banco Central de Bolivia, además de aplicar controles a nuevos escenarios y riesgos identificados en el Ente Emisor.

Asimismo, el Reglamento de Seguridad de la Información del Banco Central de Bolivia (BCB), aprobado mediante Resolución de Directorio N°122/2023 de 5 de septiembre de 2023, es una norma interna que regula las acciones y controles de seguridad destinados a proteger los activos de información del BCB, frente a riesgos y amenazas, preservando la confidencialidad, integridad y disponibilidad de la información.

4.2. Objetivo General

El objetivo del Plan Institucional de Seguridad de la información (PISI) es proteger la información del Banco Central de Bolivia (BCB) implementando controles de seguridad y mejorando la eficacia de los controles ya existentes, con base a los lineamientos y

directrices técnicas establecidos, para preservar en un nivel aceptable la confidencialidad, integridad y disponibilidad de la información Institucional.

4.2.1. Objetivos Específicos

- Identificar, clasificar y valorar los activos de información.
- Realizar la identificación, análisis y evaluación de riesgos asociados a los activos de información.
- Definir e implementar un conjunto adecuado de controles o mejorar la eficacia de los controles ya existentes a partir de los "Lineamientos para la Elaboración e Implementación de Planes Institucionales de Seguridad de la Información" de la AGETIC, en base a la aplicabilidad y los riesgos identificados.
- Regular las acciones y controles de seguridad para proteger los activos de información, en el marco del Reglamento de Seguridad de la Información del BCB.
- Monitorizar y revisar la efectividad de los controles aplicados.
- Mantener y mejorar las estrategias de seguridad de la información definidas.
- Establecer mecanismos para la gestión de incidentes en seguridad de la información para dar continuidad a las operaciones y mejorar los controles de seguridad implementados.
- Generar una cultura de seguridad de la información institucional que involucre a todo el personal del BCB mediante capacitación y concientización.

4.3. Alcance

En relación a las atribuciones del Banco Central de Bolivia (BCB), el Comité de Tecnologías y Seguridad de la Información (CTSI) definió que el alcance para el presente Plan, contemple a las áreas organizacionales de la entidad de carácter sustantivo, dichas áreas son:

- Asesoría de Política Económica (APEC)
- Gerencia de Operaciones Monetarias (GOM)
- Gerencia de Entidades Financieras (GEF)
- Gerencia de Tesorería (GTES)
- Gerencia de Operaciones Internacionales (GOI)

El presente documento, es de carácter global a todo el BCB, dado que todas las áreas organizacionales gestionan de manera integral la información en relación a la ejecución de actividades del Plan, el cumplimiento de la Política de Seguridad de la Información, entre otros.

4.4. Metodología de Gestión de Riesgos

Dentro el ámbito de seguridad de la información que contempla la gestión de riesgos y con la intención de poder alinear a un estándar, en base a las directrices dispuestas por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), el presente Plan adopta para la gestión de riesgos, la "*Guía para la metodología de gestión de riesgos*" incluida en el Anexo B de los "*Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público*", aprobados mediante Resolución Administrativa AGETIC/RA/0051/2017 de 19 de septiembre de 2017, misma que toma como referencia la Metodología de Análisis y Gestión de Riesgos MAGERIT, sin embargo, el presente Plan puede aplicar la metodología que considere adecuada para realizar la gestión de riesgos, como la que se establece en la norma ISO 27005.

En ese sentido y bajo los lineamientos dispuestos, se tomaron en cuenta y aplicaron los siguientes aspectos de la metodología:

4.4.1. Identificación, clasificación y valoración de Activos de Información

Las áreas organizacionales del BCB en coordinación con el Responsable de Seguridad de Información (RSI) identificaron, clasificaron y valoraron cada uno de los activos de información identificados en la matriz del inventario, considerando las propiedades de la información: Confidencialidad, Integridad y Disponibilidad, así como la clasificación efectuada por los Responsables de Activos de Información establecida en el Reglamento de Seguridad de la Información del BCB, dentro de uno de los siguientes niveles: Confidencial, De uso Interno y Pública.

El RSI, luego de haber gestionado la matriz del inventario de activos de información del Banco Central de Bolivia, en el marco al Reglamento de Seguridad de la Información y acorde a los Lineamientos de la AGETIC, establece que el BCB cuenta con 724 activos de información, cuyo resumen de clasificación y valoración se presentan en las siguientes tablas:

CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

ACTUALIZACIÓN DEL INVENTARIO	CLASIFICACIÓN DEL ACTIVO				TOTAL ACTIVOS
	CONFIDENCIAL	DE USO INTERNO	PÚBLICA	NO CLASIFICADO	
2da. OCTUBRE 2024	112	571	57	n/a	740
1ra. ABRIL 2024	137	511	44	n/a	692
Inicial 2018	96	217	29	293	635

Tabla 1. Clasificación de Activos de Información del BCB

VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN

ESCALA VALORACIÓN	CLASIFICACIÓN DEL ACTIVO	PROMEDIO VALORACIÓN FINAL	TOTAL ACTIVOS
MUY ALTO	Confidencial	5,00	45
	De uso interno	5,00	85
	Público	5,00	4
Promedio MUY ALTO		**5,00**	**134**
ALTO	Confidencial	4,39	53
	De uso interno	4,30	253
	Público	4,33	24
Promedio ALTO		**4,34**	**330**
MEDIO	Confidencial	3,67	8
	De uso interno	3,47	163
	Público	3,41	21
Promedio MEDIO		**3,52**	**192**
BAJA	Confidencial	2,33	2
	De uso interno	2,23	56
	Público	2,38	7
Promedio BAJA		**2,31**	**65**
MUY BAJA	Confidencial	1,42	4
	De uso interno	1,17	14
	Público	1,67	1
Promedio MUY BAJA		**1,42**	**19**
PROMEDIO GENERAL		**3,32**	**740**

Tabla 2. Valoración de Activos de Información del BCB

4.4.2. Evaluación de los Riesgos

La evaluación del riesgo permite identificar las debilidades en cuanto a controles de seguridad inexistentes o ineficaces.

Asimismo, determina y categoriza las amenazas potenciales y vulnerabilidades asociadas a los activos de información. El resultado permite la identificación de controles para reducir el nivel de los riesgos.

Habiendo identificado los principales activos, se identificó las amenazas a las que estos están expuestos. En esta fase se procede a estudiar las características de los activos para identificar puntos débiles o vulnerabilidades.

Este análisis se realiza por tipo de activo, normalmente las amenazas y vulnerabilidades comparten todos los activos que pertenecen a un tipo. Por ejemplo, los sistemas de información del BCB al estar dentro de única infraestructura tecnológica o integrada en una sola plataforma, las amenazas y vulnerabilidades son comunes.

Asimismo, se efectuó la medición del ***nivel de riesgo*** en términos de la ***probabilidad*** de que suceda el incidente (de que la amenaza se materialice) y el ***impacto*** ocasionado sobre el activo de información en las propiedades de disponibilidad, integridad y confidencialidad.

Como resultado de la valoración de los riesgos, se obtuvo que los riesgos asociados a activos de información inventariados que corresponden al nivel de riesgo "Medio", "Alto" y "Crítico".

4.4.3. Tratamiento de los Riesgos

Una vez valorado el riesgo, se eligió aquellos riesgos que superen o igualen el nivel "Medio", es decir "Crítico", "Alto" y "Medio".

El tratamiento de los riesgos establecido fue reducir el riesgo, por lo cual realizó la selección de Controles de Seguridad de la Información considerados en el Anexo A de los Lineamientos para el PISI-BCB. Es decir que, para cada riesgo, se identificó la forma en que serán tratados aplicando los controles incluidos en dicho anexo.

4.4.4. Controles Implementados y por implementar

En el Capítulo 3 del presente Plan se detalla los controles implementados y con relación a los controles a implementar como resultado de la evaluación de riesgos efectuado se tiene los siguientes controles a implementar:

1.1.1. Acuerdo de confidencialidad;
1.4. Desvinculación de personal o cambio de cargo;
2.1.2. Responsabilidad y custodia de los activos de información;
2.1.3. Uso aceptable de los activos de información;
2.2.1. Clasificación de activos de información;
2.2.2. Etiquetado y manejo de activos de información;
2.2.3. Protección del archivo;
2.3.1. Gestión de medios removibles;
3.2.1. Administración de accesos, cancelación y privilegios de usuarios;
5.1.1. Seguridad física en áreas e instalaciones;
5.1.2. Trabajo en áreas e instalaciones seguras;
5.3.1. Condiciones operativas;
6.1.2. Gestión de cambios;

6.1.3. Gestión de la Capacidad;
6.2.1. Respaldos de información;
7.1.1. Gestión de la red;
7.2.1. Mensajería y correo electrónico;
7.3.1. Transferencia de información;
8.1. Desarrollo y mantenimiento de sistemas;
8.1.6. Seguridad en base de datos;
8.2.1. Requisitos de seguridad;
9.1.1. Gestión de incidentes;
10.1. Implementación del plan de contingencias tecnológicas;
11.2.1. Evaluación de cumplimiento del plan Institucional de seguridad de la información.

4.5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI)

Siguiendo los lineamientos expresados por la AGETIC, la Política de Seguridad de la Información (PSI) del BCB, abarca los principios y posturas institucionales respecto a los dominios o ámbitos de seguridad desarrollados en el Anexo A de los Lineamientos para el PISI:

a) Seguridad en recursos humanos;
b) Gestión de activos de información;
c) Control de accesos;
d) Criptografía;
e) Seguridad física y ambiental;
f) Seguridad de las operaciones;
g) Seguridad de las comunicaciones;
h) Desarrollo, mantenimiento y adquisición de sistemas;
i) Continuidad de operaciones y gestión de incidentes de seguridad de la información;
j) Plan de contingencias tecnológicas;
k) Protección de información física documental;
l) Cumplimiento.

De acuerdo al espectro de los controles identificados en las distintas áreas sustantivas del BCB, se establece la Política de Seguridad de la Información del BCB detallada en *Anexo 2 – Política de Seguridad de la Información*, documento independiente que forma parte del presente Plan.

4.6. CRONOGRAMA DE IMPLEMENTACIÓN

El proceso de elaboración y actualización del Plan Institucional de Seguridad de la Información (PISI) del BCB, además de la aplicación de la metodología de gestión de riesgos establecida, fue actualizado el inventario de Activos de Información del Ente Emisor, actividad realizada en dos ocasiones en la gestión 2024 en aplicación de las directrices de la AGETIC y por las necesidades de acuerdo a requerimiento del Responsable de Seguridad de la Información (RSI) acorde al Reglamento de Seguridad de la Información del BCB, información documentada y respaldada. Dentro del alcance definido y la priorización de activos de información se ha realizado el análisis y evaluación de riesgos de los activos de información identificados en los escenarios de riesgos definidos, su valoración y los controles para su tratamiento.

Se priorizó la atención a los riesgos con valores críticos, altos y medios, identificados a través del análisis y evaluación de riesgo citado, obteniendo el cronograma de implementación.

4.6.1. Escenarios de riesgo de Seguridad de la Información

Los riesgos identificados dentro del Plan fueron clasificados como parte de uno de los siguientes escenarios de riesgos, definidos de acuerdo al siguiente detalle:

COD	ESCENARIO DE RIESGO	DEFINICIÓN
A.1.	Operaciones fraudulentas	Eventos que pueden ocasionar operaciones no autorizadas por manipulación de datos, de programas, configuraciones, transmisión de datos y software de base.
A.2.	Continuidad de operaciones y tecnología de Información	Eventos que impacten en la continuidad operativa e infraestructura de tecnología de información y comunicación.
A.3.	Robo, pérdida o fuga de información	Eventos que impacten en la confidencialidad y disponibilidad de activos de información.
A.4.	Oportunidad e integridad en las operaciones	Eventos que impacten en la disponibilidad e integridad de activos de información y operaciones.
A.5.	Pérdida de material monetario, monedas conmemorativas y valores	Eventos que se susciten referidos a las operaciones destinadas a la gestión de material monetario y valores en custodia.
A.6.	Proceso de Seguridad de la Información	Eventos sobre la gestión de la seguridad de la información en el BCB.
A.7.	Seguridad física y del entorno	Eventos que se presenten en áreas seguras sobre accesos no autorizados, de videovigilancia, intrusión al perímetro, desastres naturales, eventos sociales y otros escenarios referidos a áreas seguras del BCB.
A.8.	Ataques cibernéticos	Eventos de intrusión a los sistemas y servicios del BCB, generalmente por factores externos, que tengan el objetivo de dañar la imagen institucional u obtener beneficios económicos.

Tabla 3. Definición de escenarios de riesgo

4.6.2. Cronograma y Métricas e Indicadores

La implementación del presente Plan, se sujeta al cronograma de implementación de los controles definidos, mismo que no excede el plazo de un (1) año desde su aprobación, según lo establece los "*Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público*" de la AGETIC. Al respecto, el cronograma citado comprende:

- Riesgo.
- Nivel de riesgo.
- Control de seguridad aplicable.
- Actividad principal y tareas.
- Áreas organizacionales ejecutoras.
- Período de cumplimiento.
- Indicador y métrica.

Asimismo, se realizó la revisión y evaluación de los controles aplicados y por aplicar en el PISI-BCB en base al análisis de riesgos de los activos de información. Todos los controles a implementar se alinean a la Estrategia 1.14 del PEI-BCB 2021-2025.

El cronograma de implementación se detalla en el Anexo 1.

4.7. Aprobación del Plan Institucional de Seguridad de la Información

Elaboración	Revisión	Aprobación	Modificación
Daniel Abasto 18/09/2018	Comité de Tecnologías y Seguridad de la información 17/09/2018	Directorio del BCB 18/09/2018	Documento Inicial
Alfredo Lupe Copatiti 8/12/2022	Comité de Tecnologías y Seguridad de la información 29/07/2022 en Acta N° 5/2022	Directorio del BCB 15/12/2022	Actualización
Alfredo Lupe Copatiti y Yury Carlos Omar Benitez Rossel 17/01/2025	Comité de Tecnologías y Seguridad de la información 23/01/2025 en Acta N° 1/2025	Directorio del BCB 11/03/2025	Actualización

ANEXO 1
CRONOGRAMA DE IMPLEMENTACIÓN

2 – CONTINUIDAD DE OPERACIONES Y TECNOLOGÍA DE INFORMACIÓN	
Riesgo A.2.7	***Posibles ataques de seguridad al servicio web de indicadores del BCB publicado en el internet, debido a la desactualización del software de base y otras vulnerabilidades detectadas, causando daño reputacional al BCB.***
Nivel de Riesgo:	Alto
Control (AGETIC):	8.1.5 Pruebas de Seguridad
Control (ISO/IEC 27001)	8.8. Gestión de las vulnerabilidades técnicas
Actividad:	Actualizar el software de base, dar tratamiento a las vulnerabilidades detectadas e implementar mecanismos de monitoreo de eventos del servicio web de indicadores del BCB.
Tareas:	

DESCRIPCIÓN	AREA EJECUTORA	PERÍODO DE CUMPLIMIENTO
• Actualizar el software de base • Tratar las vulnerabilidades detectadas • Implementar un monitoreo de los eventos que se producen en el funcionamiento del servicio.	GSIS /GOI / GEF /RSI	Enero - Junio/2025

Indicador y métrica	
Indicador:	Servicio de indicadores actualizado.
Métrica:	Número de vulnerabilidades actualizadas sobre número total de controles vulnerabilidades detectadas.

3 –ROBO, PÉRDIDA O FUGA DE INFORMACIÓN	
Riesgo A.3.5	***Posibles ataques de intrusión a servicios y sistemas del BCB publicados en el Internet debido a la falta de revisiones de seguridad periódicas.***
Nivel de Riesgo:	Medio
Control (AGETIC):	7.1.3 Seguridad en la red perimetral
Control (ISO/IEC 27001)	8.20 Seguridad de las redes
Actividad:	Asegurar los servicios y sistemas publicados en el Internet a través de revisiones de seguridad periódicas.
Tareas:	

DESCRIPCIÓN	AREA EJECUTORA	PERÍODO DE CUMPLIMIENTO
• Identificar los servicios y sistemas publicados al internet. • Realizar la revisión de seguridad de los servicios y sistemas. • Implementar controles de seguridad y herramientas para proteger los servicios y sistemas publicados en el internet.	GSIS / RSI	Enero – Noviembre/2025

//33. R.D. N° 037/2025

3 –ROBO, PÉRDIDA O FUGA DE INFORMACIÓN			
Indicador y métrica			
Indicador:	Servicios y sistemas del BCB publicados en internet revisados.		
Métrica:	Número de servicios y sistemas revisados sobre número total de servicios y sistemas del BCB publicados en el Internet.		
Riesgo A.3.6	***Posible fuga o mal uso de la información en el sistema BCBTRAM debido a insuficientes controles en la gestión de documentos realizado por los usuarios operadores y administradores del sistema del Departamento de Gestión Documental.***		
Nivel de Riesgo:	Medio		
Control (AGETIC):	3.2.1 Administración de accesos, cancelación y privilegios de usuarios		
Control (ISO/IEC 27001)	8.2 Derechos de acceso privilegiados		
Actividad:	Revisar los registros de las operaciones de gestión de documentos en el sistema por los usuarios administradores.		
Tareas:			
DESCRIPCIÓN	**AREA EJECUTORA**	**PERÍODO DE CUMPLIMIENTO**	
• Implementar en el sistema un registro de trazabilidad de la gestión de documentos para usuarios operadores y administradores.	GSIS / SGDB / RSI	Enero – Diciembre/2025	
• Implementar la herramienta DLP en el sistema BCBTRAM.			
Indicador y métrica			
Indicador:	Los accesos privilegiados del sistema cuentan con medidas y controles adicionales de seguridad.		
Métrica:	Se tiene documentos operativos que formalizan los accesos privilegiados del sistema.		
Riesgo A.3.7	***Posible acceso no autorizado al servicio de nube y correo electrónico institucional web del BCB por suplantación de identidad y/o debilidad de contraseñas.***		
Nivel de Riesgo:	Alto		
Control (AGETIC):	3.2.1 Administración de accesos, cancelación y privilegios de usuarios. 3.2.2 Responsabilidad de los usuarios para la autenticación.		
Control (ISO/IEC 27001)	5.17 Información de autentificación		
Actividad:	implementar medidas de seguridad para reforzar el riesgo de acceso no autorizado en la nube y correo electrónico institucional web del BCB.		
Tareas:			
DESCRIPCIÓN	**AREA EJECUTORA**	**PERÍODO DE CUMPLIMIENTO**	
• Evaluar la factibilidad de autenticación de doble factor.	GSIS / RSI	Enero – Junio/2025	
• Elaborar un plan de implementación si corresponde.			
• Concientizar y capacitar al personal del BCB.			
Indicador y métrica			

3 –ROBO, PÉRDIDA O FUGA DE INFORMACIÓN		
Indicador:	Los servidores públicos están capacitados y conscientes de los riesgos de suplantación de identidad en los servicios de la nube y correo electrónico.	
Métrica:	Número de servidores públicos con capacitaciones y/o talleres cursados sobre número total de servidores públicos del BCB.	
Riesgo A.3.8	***Posible fuga, pérdida, divulgación no autorizada o mal uso de la información física y/o digital al momento de presentarse una desvinculación, cambio de cargo y/o vacación de servidores públicos debido a controles laxos en el proceso.***	
Nivel de Riesgo:	Alto	
Control (AGETIC):	1.1.1 Acuerdo de confidencialidad 1.4 Desvinculación de personal o cambio de cargo	
Control (ISO/IEC 27001)	6.6 Acuerdos de confidencialidad o no divulgación. 6.5 Responsabilidades después de la terminación o el cambio de empleo.	
Actividad:	Implementar los documentos operativos y/o herramientas de control para prevenir los riesgos de fuga, perdida, divulgación no autorizada o mal uso de la información del BCB.	
Tareas:		
DESCRIPCIÓN	**AREA EJECUTORA**	**PERÍODO DE CUMPLIMIENTO**
• Elaborar y/o actualizar el procedimiento operativo pertinente de desvinculación, cambio de cargo y/o vacación, que involucre a las áreas pertinentes, para activar las medidas de control correspondientes.	GRH / RSI	Enero – Diciembre/2025
• Las áreas involucradas en el procedimiento, deben formalizar sus procesos internos de control, en relación a las siguientes medidas de seguridad: 1. Retiro o bloqueo de medios de almacenamiento removibles. 2. Retiro o bloqueo de las credenciales de acceso otorgados para acceso a sistemas y servicios. 3. Retiro o bloqueo de los accesos otorgados en los sistemas de seguridad electrónica. 4. Efectuar la copia de respaldo de la información del equipo de computación asignado.		
• El Responsable de Seguridad de la Información debe realizar el seguimiento y control respectivo..		
Indicador y métrica		
Indicador:	Se gestiona los procesos desvinculación, cambio de cargo y/o vacación que controla los riesgos de la seguridad de la información.	
Métrica:	Número de documentos operativos implementados.	
Riesgo A.3.9	***Posible divulgación no autorizada, fuga o pérdida de información a través de los medios de almacenamiento removibles por falta de controles adecuados y***	

3 –ROBO, PÉRDIDA O FUGA DE INFORMACIÓN			
	manejo inadecuado de la información digital procesada e histórica en las áreas del BCB.		
Nivel de Riesgo:	Alto		
Control (AGETIC):	2.1.3 Uso aceptable de los activos de información 2.3.1 Gestión de medios removibles		
Control (ISO/IEC 27001)	5.10 Uso aceptable de la información y otros activos asociados. 7.10 Medios de almacenamiento.		
Actividad:	Implementar controles normativos y tecnológicos para minimizar el riesgo de uso, divulgación no autorizada, fuga o pérdida de información digital del BCB.		
Tareas:			
DESCRIPCIÓN	**AREA EJECUTORA**	**PERÍODO DE CUMPLIMIENTO**	
• Elaborar documentos operativos para el uso de medios de almacenamiento removibles tanto al interior como exterior del BCB. • Mejorar e Implementar controles tecnológicos para el uso de medios de almacenamiento removibles. • Mejorar e Implementar mecanismos de monitoreo de acuerdo a la clasificación de información. • Evaluar y establecer reglas de uso correcto de la información digital dentro y fuera del BCB.	GSIS / RSI	Enero – Diciembre/2025	
Indicador y métrica			
Indicador:	El uso correcto de los medios de almacenamiento removibles dentro y fuera del BCB se encuentra gestionado.		
Métrica:	Número de documentos operativos para el uso correcto de los medios de almacenamiento removibles implementado.		
Riesgo A.3.10	***Posible fuga o mal uso de la información del BCB mediante uso de dispositivos móviles de propiedad de los servidores públicos debido a la escasa normativa y controles técnicos sobre el uso de dichos dispositivos en el BCB.***		
Nivel de Riesgo:	Medio		
Control (AGETIC):	3.3.3 Acceso de dispositivos móviles		
Control (ISO/IEC 27001)	8.1 Dispositivos de punto final de usuario 6.7 Trabajo remoto		
Actividad:	Establecer lineamientos de las condiciones de uso de dispositivos móviles de propiedad de los servidores públicos e implementar medidas de control tecnológicos para contar con el registro, control de software y monitoreo de uso.		
Tareas:			
DESCRIPCIÓN	**AREA EJECUTORA**	**PERÍODO DE CUMPLIMIENTO**	
• Elaborar un documento operativo para establecer lineamientos de condiciones de uso de dispositivos móviles. • Evaluar y actualizar procedimiento de acceso a la red wifi del BCB	GSIS / RSI	Enero – Octubre/2025	

3 –ROBO, PÉRDIDA O FUGA DE INFORMACIÓN		
• Elaborar un propuesta de un mecanismo de monitoreo de uso de dispositivos móviles.		
Indicador y métrica		
Indicador:	Se cuenta con documentos normativos sobre uso de dispositivos móviles	
Métrica:	Numero de documentos normativos implementados sobre el número de documentos normativos elaborados sobre uso de dispositivos móviles.	

4 – OPORTUNIDAD E INTEGRIDAD EN LAS OPERACIONES		
Riesgo A.4.5	***Posible acceso no autorizados a los sistemas de seguridad electrónica por falta de gestión formal de la administración de credenciales de acceso.***	
Nivel de Riesgo:	Alto	
Control (AGETIC):	3.2.1 Administración de accesos, cancelación y privilegios de usuarios	
Control (ISO/IEC 27001)	8.2 Derechos de acceso privilegiado 5.18 Derechos de acceso	
Actividad:	Asegurar la gestión de control de accesos y perfiles del sistema de seguridad electrónica.	
Tareas:		
DESCRIPCIÓN	**AREA EJECUTORA**	**PERÍODO DE CUMPLIMIENTO**
• Elaborar documento operativo para gestionar de credenciales de acceso del sistema de seguridad electrónica	SGR / RSI	Enero – Diciembre/2025
• Contar con un reporte credenciales de acceso en relación a las siguientes operaciones: 1. Autorizaciones. 2. Asignación de roles. 3. Trazabilidad de ingresos y salidas.		
Indicador y métrica		
Indicador:	El control de accesos y perfiles de los sistemas de seguridad electrónica se encuentran gestionados.	
Métrica:	Número de sistemas de seguridad electrónica gestionados con control de accesos y perfiles sobre el número total de sistemas de seguridad electrónica.	

7 – SEGURIDAD FÍSICA Y DEL ENTORNO	
Riesgo A.7.4	***Acceso no autorizado a las áreas seguras.***
Nivel de Riesgo:	Alto
Control (AGETIC):	5.1.1 Seguridad física en áreas e instalaciones
Control (ISO/IEC 27001)	7.1 Perímetro de seguridad física 7.2 Entrada física
Actividad:	Asegurar la gestión de control de accesos y perfiles del sistema de seguridad electrónica.
Tareas:	

//37. R.D. N° 037/2025

7 – SEGURIDAD FÍSICA Y DEL ENTORNO		
DESCRIPCIÓN	**AREA EJECUTORA**	**PERÍODO DE CUMPLIMIENTO**
• Elaborar normativa de control de accesos. • Identificar las áreas e instalaciones consideradas seguras. • Elaborar procedimientos de acceso a las diferentes áreas críticas según las características de seguridad de la información. • Implementar mecanismos de acceso físico para áreas seguras. • Señalizar las áreas e instalaciones seguras. • Instalar sistemas de monitoreo y vigilancia. • Elaborar procedimientos para la obtención y entrega de grabaciones de los sistemas de monitoreo y vigilancia. • *Implementar mecanismos de alerta al interior y exterior de las instalaciones seguras ante ocurrencias de eventos de seguridad.* • Realizar simulacros de evacuación y respuesta ante amenazas internas, externas, ambientales y/o revueltas sociales. • Contar con señalética visible para evacuaciones o contingencias.	SGR / RSI	Enero – Junio/2025 (Se amplía el Plazo para la complementación de actividades y mejoramiento de las tareas ya implementadas)
Indicador y métrica		
Indicador:	El control de accesos a las áreas seguras del BCB se encuentran gestionados.	
Métrica:	Número de áreas seguras que cuentan con control de acceso sobre el número total de áreas seguras del BCB.	
Riesgo A.7.6	***Posible pérdida de información de los recintos de archivos de las áreas del BCB por insuficientes medidas de protección de controles de acceso y/o videovigilancia.***	
Nivel de Riesgo:	Alto	
Control (AGETIC):	2.2.3 Protección de archivo	
Control (ISO/IEC 27001)	7.1 Perímetro de seguridad física 7.2 Entrada física	
Actividad:	Implementar medidas de seguridad en los recintos de archivo de oficinas de las áreas del BCB.	
Tareas:		
DESCRIPCIÓN	**AREA EJECUTORA**	**PERÍODO DE CUMPLIMIENTO**
• Evaluar el estado actual de medidas de protección de los archivos de oficina del BCB	SGR / RSI	Enero – Diciembre/2025

7 – SEGURIDAD FÍSICA Y DEL ENTORNO		
• Implementar los controles de seguridad de acceso y videovigilancia en coordinación con las áreas Responsables.		
Indicador y métrica		
Indicador:	Los archivos de las áreas del BCB se encuentran cuentan con medidas de seguridad física.	
Métrica:	Número de áreas de archivo que cuentan con seguridad física sobre el número total de archivos de áreas del BCB.	

8 – ATAQUES CIBERNÉTICOS		
Riesgo A.8.1	***Posible secuestro de datos e información del BCB por ataques de Ciberseguridad a través de malware por correo electrónico.***	
Nivel de Riesgo:	Medio	
Control (AGETIC):	6.2.1 Respaldos de información. 7.2.1 Mensajería y correo electrónico.	
Control (ISO/IEC 27001)	8.13 Copia de seguridad de la Información. 8.7 Protección contra malware.	
Actividad:	Mejorar e Implementar herramientas tecnológicas y de concientización para la protección ante robo, fuga y cifrado de datos del BCB.	
Tareas:		
DESCRIPCIÓN	**AREA EJECUTORA**	**PERÍODO DE CUMPLIMIENTO**
• Proponer medidas y controles efectivos para fortalecer la seguridad.	GSIS / RSI	Enero – Diciembre/2025
• Verificar y probar la implementación de copias de seguridad cifradas y sin conexión de los sistemas, bases de datos e información crítica del BCB.		
• Implementar planes de concientización para fortalecer las habilidades y madurez de la cultura institucional en ciberseguridad.		
Indicador y métrica		
Indicador:	La información crítica del BCB está protegida contra incidentes del tipo ransonware.	
Métrica:	Número de eventos de malware detectados sobre total de eventos registrados en las herramientas de seguridad.	

ANEXO 2
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI)

La Política de Seguridad de la Información (PSI), se encuentra en documento separado y aprobado por las instancias respectivas, el mismo que forma parte integrante e indivisible del presente Plan.

//39. R.D. N° 037/2025

BICENTENARIO DE BOLIVIA | BANCO CENTRAL DE BOLIVIA | ESTADO PLURINACIONAL DE BOLIVIA

ANEXO 2

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

(PSI-BCB)

Banco Central de Bolivia

VERSIÓN 3.0 GESTIÓN 2025	ELABORADO POR: *Responsable de Seguridad de la Información*
	APROBADO POR: *Directorio del Banco Central de Bolivia*

//40. R.D. N° 037/2025

BICENTENARIO DE BOLIVIA | BANCO CENTRAL DE BOLIVIA | ESTADO PLURINACIONAL DE BOLIVIA

INDICE GENERAL

INTRODUCCIÓN

El Banco Central de Bolivia (BCB) destaca a la información institucional como un activo de alta importancia que posibilita el cumplimiento de sus objetivos, por lo cual existe la necesidad de implementar medidas de protección de la información del BCB.

Para el BCB, la gestión de la seguridad de la información busca la disminución del impacto generado sobre sus activos de información, por los riesgos identificados de manera sistemática con objeto de mantener un nivel aceptable de la integridad, confidencialidad y la disponibilidad de la misma.

En ese sentido, la Política de Seguridad de la Información (PSI), establece directrices que permiten definir estrategias para la protección de los activos de información ante amenazas que pudieran afectar su disponibilidad, integridad y confidencialidad, además del desarrollo de planes de continuidad de los sistemas de información, gestión de los riesgos y la respectiva implementación de los controles de seguridad de la información por parte del personal del BCB.

Para este fin, se cuenta con el compromiso de la Máxima Autoridad Ejecutiva de la Institución, Directores, Asesor, Gerentes, Subgerentes, Jefes de Departamento y del personal de todas las Áreas y Unidades Organizacionales para la adopción, difusión, consolidación y cumplimiento de la presente Política.

TÉRMINOS Y DEFINICIONES

Los siguientes términos y definiciones son aplicables para el propósito del presente documento:

Activo de información: Conocimiento o información que tiene valor para la institución.

Amenaza: Causa potencial de un incidente no deseado, que puede afectar la seguridad de la información. Se trata de un factor externo al activo de información, del que no se tiene control.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a personas o procesos no autorizados.

Disponibilidad: Propiedad de la información de ser accesible y utilizable para los usuarios autorizados.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Integridad de la información: Propiedad que salvaguarda la exactitud y completitud de la información.

Plan Institucional de Seguridad de la Información (PISI): Documento que establece las actividades relativas a la organización y gestión de la seguridad de la información en la Entidad.

Política de Seguridad de la Información (PSI): Acciones o directrices que establecen la postura institucional en relación a la seguridad de la información, incluidas dentro del Plan Institucional de Seguridad de la Información.

Responsable del Activo de Información: Es la Máxima Autoridad de Área (MAA) que tiene la responsabilidad y atribución de establecer los controles, políticas y directrices de seguridad de la información relacionada al activo de información enmarcado al proceso del cual es responsable.

Riesgo de seguridad de la Información: Probabilidad de que una amenaza aproveche vulnerabilidades de un activo de información y provoque impacto.

Seguridad de la información: Protección de los activos de información frente a las amenazas que puedan afectar a su confidencialidad, integridad o disponibilidad.

Vulnerabilidad: Debilidad de un activo de información o control de seguridad que puede ser aprovechada por una amenaza. Es un factor interno del que se tiene control.

OBJETIVO GENERAL

Establecer las directrices que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información del BCB, teniendo en cuenta los objetivos, los procesos, las operaciones y los requisitos legales vigentes en la Entidad.

OBJETIVOS ESPECÍFICOS

- Puntualizar las políticas relacionadas con el análisis de riesgos e identificación de controles en los dominios relevantes.
- Fortalecer la concientización de la importancia de la seguridad de la información del BCB en el personal.

BICENTENARIO DE BOLIVIA | BANCO CENTRAL DE BOLIVIA | ESTADO PLURINACIONAL DE BOLIVIA

- Establecer políticas, reglamentos y procedimientos en materia de seguridad de la información
- Procurar la mejora continua de la continuidad de operaciones del BCB frente a amenazas de diferente índole.

ALCANCE

La Política de Seguridad de la Información es aplicable a todas las áreas y unidades organizacionales del BCB, a sus recursos, a los procesos internos o externos y a todo el personal de la entidad, cualquiera sea su situación laboral y el tipo de tareas que desempeñen.

ROLES Y RESPONSABILIDADES

a) El **Comité de Tecnología y Seguridad de la Información (CTSI)** es responsable proponer al Directorio del BCB la aprobación de la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
b) La **Máxima Autoridad de Área (MAA)** es responsable de cumplir y hacer cumplir la PSI y la normativa que se deprenda de ella al interior de su área.
c) El **Responsable de Seguridad de la Información (RSI)** es el encargado de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información. Asimismo, tiene la función de proponer la Política de Seguridad de la Información.
d) La **Gerencia de Sistemas**, es responsable de cumplir funciones relativas a la seguridad informática de la entidad.
e) La **Gerencia de Recursos Humanos** es responsable de promover la concientización y formación del recurso humano del BCB en seguridad de la información.
f) La **Gerencia de Asuntos Legales** es responsable de asesorar en materia legal en lo que se refiere a la seguridad de la información.
g) La **Gerencia de Auditoria Interna** es responsable de llevar a cabo auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos y tecnología de información.
h) Todo el **personal del BCB**, es responsable de conocer y cumplir la PSI vigente.

DESARROLLO

La Política de Seguridad de la Información del BCB, se sustenta en el resguardo, protección y seguridad de la información que se genera, procesa y almacena. A este efecto, se ha definido un conjunto de directrices de alto nivel que permiten preservar la confidencialidad, disponibilidad e integridad de la información.

El Banco Central de Bolivia:

1. Establece que la información que genera, procesa y resguarda es de gran importancia para el ejercicio de sus atribuciones constitucionales y las establecidas en la ley 1670.
2. Protege los activos de información, orientando sus esfuerzos a la preservación de la confidencialidad, integridad y disponibilidad de la información institucional, alineado al plan estratégico institucional (PEI).

En relación a los dominios de la seguridad el BCB establece las siguientes políticas:

Dominio de Seguridad / Descripción	Postura Institucional
a) Seguridad en recursos humanos Es necesario establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y el BCB con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral.	a) Respecto a la protección de la información institucional ante amenazas que se originan de parte del recurso humano del BCB. 1. Proteger la información del BCB de las amenazas originadas de parte del Servidor(a) Público(a). 2. Concientizar, entrenar y capacitar a los servidores públicos para adoptar una cultura de seguridad de la información. 3. Establecer responsabilidades y obligaciones para manejo de la información a la que tienen acceso los Servidores Públicos y terceros; durante y después del vínculo laboral. 4. Dar cumplimiento al compromiso de confidencialidad de servidoras y servidores públicos y uso adecuado de los servicios y recursos del BCB.
b) Gestión de activos de información Con el fin de preservar la integridad, disponibilidad y confidencialidad de los activos de información, se debe administrar, controlar y	b) Respecto al uso y protección de activos de información. 5. Identificar y clasificar los activos de información en físico y digital, a fin determinar las amenazas y vulnerabilidades.

Dominio de Seguridad / Descripción	Postura Institucional
asignar responsabilidades en el uso y protección de los mismos	6. Aplicar controles de seguridad de la información de acuerdo a la clasificación que establezca el BCB. 7. Priorizar la implementación de controles tecnológicos, de infraestructura y recursos humanos para la adecuada protección de los activos de la información y gestión de medios de almacenamiento removibles.
c) Control de accesos Gestionar los accesos a servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario.	c) Respecto al control de accesos a recursos de red, información, sistemas y aplicaciones. 8. Gestionar el acceso a los recursos de red, información, sistemas y aplicaciones, sistemas provistos por terceros, incluyendo el teletrabajo, estableciendo los niveles de autorización y mecanismos de protección acordes a la clasificación de activos de información. 9. Gestionar los accesos a recursos de red, información, sistemas y aplicaciones de acuerdo a las funciones.
d) Criptografía El uso de técnicas criptográficas aporta mayores niveles de seguridad para proteger la confidencialidad, autenticidad e integridad de la información, además del no repudio y autenticación.	d) Respecto a la protección de información transmitida a través de redes de comunicaciones 10. Aplicar mecanismos criptográficos para la protección, transmisión y resguardo de información acorde a la sensibilidad y criticidad de la misma.
e) Seguridad física y ambiental Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica para el BCB, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.	e) Respecto a la protección de áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica 11. Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos del BCB. 12. Clasificar áreas e instalaciones en función a su sensibilidad y criticidad, implementar controles de acceso físico, video vigilancia y señalética. 13. Disponer de elementos de seguridad para mitigar o transferir riesgos de origen natural, tecnológico o provocado por las personas. 14. No permitir el ingreso y trabajo no supervisado de terceras personas y/o servidores públicos ajenos a los ambientes restringidos, áreas e instalaciones seguras o

Dominio de Seguridad / Descripción	Postura Institucional
	críticas, para evitar posibles incidentes de seguridad. 15. Contar con equipamiento para mitigar posibles incendios y mecanismos de alerta al interior y/o exterior de las instalaciones, ante la ocurrencia de eventos de seguridad. 16. Cumplir con los procedimientos operativos internos y normativa vigente del BCB, para asegurar y garantizar que el personal externo o terceros que desee ingresar a las áreas y/o ambientes restringidos, áreas e instalaciones seguras o críticas del BCB, cuente con la debida autorización de las Máximas Autoridades de Área según sus responsabilidades. 17. Controlar que el personal externo o terceros, ajenos al BCB, porten su identificación y se autentifique su identidad al ingreso y salida de la institución.
f) Seguridad de las operaciones Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta.	f) Respecto a la seguridad de las operaciones 18. Implementar controles para asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta y continua, considerando la responsabilidad para la ejecución de las operaciones, protección contra pérdida de información, generación de copias de respaldos y resguardo de la información. 19. Implementar y fortalecer las herramientas tecnológicas y controles ante ataques cibernéticos.
g) Seguridad de las comunicaciones Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos.	g) Respecto a la seguridad de las comunicaciones 20. Implementar mecanismos de protección para la disponibilidad de la información en las redes de datos. 21. Gestionar de forma eficiente y segura el servicio de mensajería y correo electrónico y preservando la integridad y confidencialidad de la información transferida.
h) Desarrollo, mantenimiento y adquisición de sistemas Establecer requisitos de seguridad para el desarrollo, mantenimiento y adquisición de sistemas que consideren pruebas de seguridad,	h) Respecto a la seguridad en el ciclo de vida de los sistemas y/o software que se desarrolle y/o adquiera 22. Establecer e implantar requisitos de seguridad en el ciclo de vida de los sistemas,

BICENTENARIO DE BOLIVIA | BANCO CENTRAL DE BOLIVIA | ESTADO PLURINACIONAL DE BOLIVIA

Dominio de Seguridad / Descripción	Postura Institucional
pruebas de calidad y aceptación para desarrollos internos y externos.	sean software vigentes o en proceso de implementación.
i) Continuidad de operaciones y gestión de incidentes de seguridad de la información Establecer mecanismos para la gestión de incidentes en seguridad de la información dentro del BCB para dar continuidad a las operaciones y mejorar los controles de seguridad implementados.	i) Respecto a la continuidad de las operaciones y procesos mediante la gestión de incidentes en seguridad de la información. 23. Contar con recursos tecnológicos, humanos, infraestructura física y normativa para permitir la continuidad operativa de los procesos críticos. 24. Implementar, mantener y probar el Plan de Continuidad Operativa. 25. Gestionar los incidentes de seguridad de la información que afecten la seguridad mediante herramientas adecuadas. 26. Gestionar los incidentes de seguridad de la información abarcando la prevención, detección, respuesta y recuperación.
j) Plan de contingencias tecnológicas Implementar un Plan de Contingencias Tecnológicas que permita controlar un incidente de seguridad de la información o una situación de emergencia, minimizando sus consecuencias negativas. Asimismo deberá determinar sus requisitos para la seguridad de la información ante situaciones adversas.	j) Respecto al Plan de contingencias tecnológicas. 27. Contar con un Plan de Contingencias Tecnológicas formalizado, actualizado e implementado donde se asignará responsabilidades para su ejecución a los propietarios de los activos de información.
k) Protección de información física documental Gestionar la seguridad de la información física documental de manera integral.	k) Respecto a la protección de información física documental 28. Evitar el robo, pérdida o modificación de documentos físicos mediante su resguardo seguro.
l) Cumplimiento Asegurar el cumplimiento operativo del Plan Institucional de Seguridad de la Información que conlleva la Política de Seguridad y la documentación resultante de la misma	l) Respecto al cumplimiento 29. Revisar los controles evaluando periódicamente el cumplimiento de la normativa documental del Plan Institucional de Seguridad de la Información, verificando que los mismos se encuentran en operación. Asimismo, efectuar auditorías al Plan Institucional de Seguridad de la Información.

//48. R.D. N° 037/2025

DIFUSIÓN

El Responsable de Seguridad de la Información (RSI), a través de la Gerencia General, es el encargado de difundir las políticas de seguridad de la información del BCB a todo el personal. Este documento deberá ser de libre acceso a través de la red intranet del BCB.

CUMPLIMIENTO

La presente Política de Seguridad de la Información es de cumplimiento obligatorio por todo el personal del BCB.

SANCIONES

El incumplimiento a las políticas de seguridad de la información del BCB, ya sea de forma intencional o por negligencia, será sancionado de acuerdo a normativa vigente.

HISTÓRICO DE CAMBIOS

Elaboración	Revisión	Aprobación	Modificación
Daniel Abasto 18/09/2018	Comité de Tecnologías y Seguridad de la información 17/09/2018	Directorio del BCB 18/09/2018	Documento Inicial
Alfredo Lupe Copatiti 8/12/2022	Comité de Tecnologías y Seguridad de la información 29/07/2022 en Acta N° 5/2022	Directorio del BCB 15/12/2022	Actualización
Alfredo Lupe Copatiti y Yury Carlos Omar Benitez Rossel 17/01/2025	Comité de Tecnologías y Seguridad de la información 23/01/2025 en Acta N° 1/2025	Directorio del BCB 11/03/2025	Actualización