

COPIA LEGALIZADA



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA



DIRECTORIO

/39. R.D. N° 037/2025



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: <i>Responsable de Seguridad de la Información</i>
	APROBADO POR: <i>Directorio del Banco Central de Bolivia</i>



"2025 BICENTENARIO DE BOLIVIA"



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA



DIRECTORIO

//40. R.D. N° 037/2025



Banco Central de Bolivia

Política de Seguridad de la Información

INDICE GENERAL

Introducción	3
Términos y Definiciones.....	3
Objetivo General	4
Objetivos Específicos.....	4
Alcance	5
Roles y Responsabilidades	5
Desarrollo	6
Difusión	10
Cumplimiento	10
Sanciones	10
Histórico de Cambios	10

266 10



"2025 BICENTENARIO DE BOLIVIA"



DIRECTORIO

//41. R.D. N° 037/2025

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.



COPIA LEGALIZADA



BANCO
CENTRAL DE
BOLIVIA



DIRECTORIO

//42. R.D. N° 037/2025



BANCO
CENTRAL DE
BOLIVIA



Banco Central de Bolivia

Política de Seguridad de la Información

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.

4 de 10



"2025 BICENTENARIO DE BOLIVIA"

DIRECTORIO

//43. R.D. N° 037/2025


**ESTADO PLURINACIONAL DE
BOLIVIA**
*Banco Central de Bolivia**Política de Seguridad de la Información*

- 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 Auditoría 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.



5 de 10

**"2025 BICENTENARIO DE BOLIVIA"**

COPIA LEGALIZADA



BANCO
CENTRAL DE
BOLIVIA

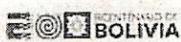


ESTADO PLURINACIONAL DE
BOLIVIA



DIRECTORIO

//44. R.D. N° 037/2025



BANCO
CENTRAL DE
BOLIVIA



Banco Central de Bolivia

Política de Seguridad de la Información

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 <p>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.</p>	a) <u>Respecto a la protección de la información institucional ante amenazas que se originan de parte del recurso humano del BCB.</u> <ol style="list-style-type: none">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 <p>Con el fin de preservar la integridad, disponibilidad y confidencialidad de los activos de información, se debe administrar, controlar y</p>	b) <u>Respecto al uso y protección de activos de información.</u> <ol style="list-style-type: none">5. Identificar y clasificar los activos de información en físico y digital, a fin determinar las amenazas y vulnerabilidades.

5 de 10



"2025 BICENTENARIO DE BOLIVIA"


DIRECTORIO

//45. R.D. N° 037/2025



Dominio de Seguridad / Descripción	Postura Institucional
asignar responsabilidades en el uso y protección de los mismos	<p>6. Aplicar controles de seguridad de la información de acuerdo a la clasificación que establezca el BCB.</p> <p>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.</p>
c) Control de accesos Gestionar los accesos a servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario.	<p>c) <u>Respecto al control de accesos a recursos de red, información, sistemas y aplicaciones.</u></p> <p>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.</p> <p>9. Gestionar los accesos a recursos de red, información, sistemas y aplicaciones de acuerdo a las funciones.</p>
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 reudio y autenticación.	<p>d) <u>Respecto a la protección de información transmitida a través de redes de comunicaciones</u></p> <p>10. Aplicar mecanismos criptográficos para la protección, transmisión y resguardo de información acorde a la sensibilidad y criticidad de la misma</p>
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.	<p>e) <u>Respecto a la protección de áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica</u></p> <p>11. Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos del BCB.</p> <p>12. Clasificar áreas e instalaciones en función a su sensibilidad y criticidad, implementar controles de acceso físico, video vigilancia y señalética.</p> <p>13. Disponer de elementos de seguridad para mitigar o transferir riesgos de origen natural, tecnológico o provocado por las personas.</p> <p>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</p>




DIRECTORIO

//46. R.D. N° 037/2025



Dominio de Seguridad / Descripción	Postura Institucional
	<p>críticas, para evitar posibles incidentes de seguridad.</p> <p>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.</p> <p>16. Cumplir con los procedimientos operativos internos y normativa vigente del BCB, para asegurar y garantizar que el personal externo o tercero que deseé 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.</p> <p>17. Controlar que el personal externo o tercero, ajeno al BCB, porten su identificación y se autentifique su identidad al ingreso y salida de la institución.</p>
f) Seguridad de las operaciones Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta.	f) Respeto 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.
g) Seguridad de las comunicaciones Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos.	g) Respeto a la seguridad de las comunicaciones 19. Implementar y fortalecer las herramientas tecnológicas y controles ante ataques cibernéticos. 20. Implementar mecanismos de protección para la disponibilidad de la información en las redes de datos.
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) Respeto a la seguridad en el ciclo de vida de los sistemas y/o software que se desarrolle y/o adquiera 21. Gestionar de forma eficiente y segura el servicio de mensajería y correo electrónico y preservando la integridad y confidencialidad de la información transferida. 22. Establecer e implantar requisitos de seguridad en el ciclo de vida de los sistemas.

DIRECTORIO

//47. R.D. N° 037/2025

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.	<u>i) Respeto a la continuidad de las operaciones y procesos mediante la gestión de incidentes en seguridad de la información.</u> 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.	<u>j) Respeto al Plan de contingencias tecnológicas.</u> 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.	<u>k) Respeto a la protección de información física documental</u> 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 conllevará la Política de Seguridad y la documentación resultante de la misma	<u>l) Respeto al cumplimiento</u> 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.



**DIRECTORIO**

//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 Benítez 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