



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

RESOLUCIÓN DE DIRECTORIO N° 122/2023

ASUNTO: GERENCIA GENERAL – APROBAR EL REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN DEL BCB.

VISTOS:

La Constitución Política del Estado, de 7 de febrero de 2009.

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

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

El Decreto Supremo N° 1793 de 13 de noviembre de 2013.

El Decreto Supremo N° 2514 de 9 de septiembre de 2015.

El Estatuto del Banco Central de Bolivia, aprobado mediante Resolución de Directorio N° 095/2022 de 6 de octubre de 2022.

La Resolución Administrativa AGETIC/RA/0051/2017 de 19 septiembre de 2017, modificada por la Resolución Administrativa AGETIC/RA/0059/2018 de 1 agosto de 2018.

La Resolución Administrativa AGETIC/RA/0068/2018 de 7 de septiembre de 2018.

Resolución de Directorio N° 121/2022 de 15 de diciembre de 2022, aprueba el Plan Institucional de Seguridad de la Información del BCB.

El Informe BCB-SGR-RSI-INF-2023-32 de 1 de septiembre de 2023, emitido por la Subgerencia Gestión de Riesgos (SGR).

El Informe BCB-GAL-SANO-DLBCI-INF-2023-298 de 4 de septiembre de 2023, emitido por la Gerencia de Asuntos Legales (GAL).

CONSIDERANDO:

Que el Artículo 327 de la Constitución Política del Estado establece que el BCB es una institución de derecho público, con personalidad jurídica y patrimonio propio. En el marco de la política económica del Estado, es función del BCB mantener la estabilidad del poder



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//2. R.D. N° 122/2023

adquisitivo interno de la moneda, para contribuir al desarrollo económico y social.

Que el Artículo 1 de la Ley 1670 dispone que el BCB 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 y por ello órgano rector del sistema de intermediación financiera nacional, con competencia administrativa, técnica y financiera y facultades normativas especializadas de aplicación general, en la forma y, con los alcances establecidos en la presente Ley.

Que el Artículo 44 de la Ley N° 1670 del BCB, establece que la Máxima Autoridad del Banco Central de Bolivia 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 los incisos a) y o) del Artículo 54 de la Ley N° 1670 del BCB, que establecen que son atribuciones del Directorio del BCB el dictar normas y adoptar las decisiones generales que fueran necesarias para que el BCB cumpla las funciones, competencias y facultades que le asigna la Ley; así como aprobar, modificar e interpretar el Estatuto y Reglamentos del BCB, por dos tercios de votos de la totalidad de sus miembros, sin necesidad de ningún acto administrativo adicional.

Que el párrafo 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 los usuarios y usuarias, 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 párrafo II del Artículo 4 del Reglamento a la Ley N° 164 aprobado por el Decreto Supremo N° 1793 de 13 de noviembre de 2013, determina que se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//3. R.D. N° 122/2023

Que el Artículo 8 del Decreto Supremo N° 1793, establece que las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad.

Que el Artículo 1 del Decreto Supremo N° 2514, establece la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).

Que el Artículo 7 del Decreto Supremo N° 2514, establece como función de la AGETIC el establecer los lineamientos técnicos en seguridad de información para las entidades del sector público.

Que la Resolución Administrativa AGETIC/RA/0051/2017, aprueba los “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público”.

Que la Resolución Administrativa AGETIC/RA/0068/2018, aprueba los “Lineamientos para la elaboración e implementación de los Planes de Contingencia Tecnológica en entidades del sector público.”

Que los numerales 1) y 30) del Artículo 10 del Estatuto del BCB, determinan como atribuciones del Directorio, aprobar las decisiones generales y dictar las normas que fueren necesarias para que el BCB cumpla las funciones, competencias y facultades que le asigna la Ley; definir las políticas del BCB, normativas especializadas de aplicación general y normas internas, así como efectuar el seguimiento de su ejecución; además de aprobar, modificar e interpretar el Estatuto y Reglamentos del BCB, por dos tercios de votos de la totalidad de sus miembros, sin necesidad de acto administrativo adicional.

Que el párrafo I del Artículo 24 del Estatuto del BCB, dispone que las resoluciones y decisiones del Directorio se adoptan por simple mayoría de votos de sus miembros presentes en reunión, salvo los casos en que la Ley N° 1670 o este Estatuto exijan mayorías calificadas.

Que el Artículo 26 del Estatuto del BCB, establece que el Directorio se pronuncia sobre los asuntos de su competencia mediante resoluciones. También puede hacerlo mediante decisiones que constarán expresamente en Acta. Asimismo, todo proyecto de Resolución de Directorio debe ser motivado y justificado por un informe técnico de la Gerencia o Gerencias



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//4. R.D. N° 122/2023

a las que corresponde el asunto objeto de la resolución y por un informe de la Gerencia de Asuntos Legales. Estos informes deberán ser remitidos a Directorio por intermedio de la Gerencia General con su recomendación.

Que la Resolución de Directorio N° 121/2022 de 15 de diciembre de 2022, aprueba el Plan Institucional de Seguridad de la Información del BCB.

Que el Informe de la Subgerencia de Gestión de Riesgos BCB-SGR-RSI-INF-2023-32, concluye que el proyecto de Reglamento de Seguridad de la Información del Banco Central de Bolivia es necesario para dar cumplimiento con el Plan Institucional de Seguridad de la Información (PISI-BCB) y la Política de Seguridad de la Información del BCB donde se regule la gestión de activos de información, gestión de accesos, la seguridad física y ambiental, el desarrollo y mantenimiento de sistemas, el correo electrónico institucional, el uso de la criptografía, la seguridad en el teletrabajo, la seguridad de las comunicaciones y servicios de red, la gestión de incidentes de seguridad y la seguridad de la información en físico conforme al contexto normativo y operativo actual del BCB. En este sentido, el Reglamento de Seguridad de la Información propuesto cuenta con la justificación y viabilidad técnica, por lo que recomienda al Directorio su aprobación.

Que el Informe de la Gerencia de Asuntos Legales BCB-GAL-SANO-DLBCI-INF-2023-298, concluye que el contenido de la propuesta de Reglamento de Seguridad de la Información del BCB, propuesto por la SGR es viable legalmente, toda vez que no contraviene el ordenamiento jurídico, recomendando al Directorio del Ente Emisor su aprobación.

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

Artículo 1.- Aprobar el Reglamento de Seguridad de la Información del BCB, en sus doce (XII) Capítulos, treinta y siete (37) Artículos y una (1) Disposición Final Única que en anexo forman parte de esta Resolución.

Artículo 2.- La presente resolución entrará en vigencia a partir de su publicación.





BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//5. R.D. N° 122/2023

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

La Paz, 5 de septiembre de 2023

FDO. ROGER EDWIN ROJAS ULO, Oscar Ferrufino Morro, Gabriel Herbas Camacho, Gumercindo Héctor Pino Guzmán, Diego Alejandro Pérez Cueto Eulert.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//6. R.D. N° 122/2023

ANEXO

REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN DEL BANCO CENTRAL DE BOLIVIA

CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1. (Objeto)

El presente Reglamento tiene por objeto regular las acciones y controles de seguridad destinados a proteger los activos de información del Banco Central de Bolivia, frente a riesgos y amenazas, manteniendo la confidencialidad, integridad y disponibilidad de la información.

Artículo 2. (Ámbito de aplicación)

El presente Reglamento es de aplicación y cumplimiento obligatorio para las servidoras y servidores públicos, así como los consultores y otros que hagan uso de los activos de información del Banco Central de Bolivia, denominados en adelante como usuarios.

Artículo 3. (Abreviaturas)

Para fines de interpretación del presente Reglamento, se establecen las siguientes abreviaturas:

- a) **BCB:** Banco Central de Bolivia.
- b) **RSI:** Responsable de Seguridad de la Información.
- c) **GSIS:** Gerencia de Sistemas.
- d) **SGR:** Subgerencia de Gestión de Riesgos.
- e) **DSCI:** Departamento de Seguridad y Continuidad Informática.
- f) **MAA:** Máxima Autoridad de Área.
- g) **CPD:** Centro de Procesamiento de Datos.
- h) **AGETIC:** Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//7. R.D. N° 122/2023

Artículo 4. (Definiciones)

Para la aplicación del presente Reglamento, se establecen las siguientes definiciones que aplican a la información digital y/o en físico:

- a) **Activo de información:** Se refiere a toda información o elemento relacionado con el tratamiento de esta (sistemas, soportes, documentos en papel, personas).
- b) **Área administradora del sistema:** Área diferente a la GSIS, responsable de administrar y mantener sistemas de información especializados.
- c) **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.
- d) **Áreas seguras:** Recintos donde se genera, procesa, transmite o almacena información del BCB.
- e) **Autenticación:** Proceso por el cual el usuario se identifica de forma inequívoca para comprobar que es quién dice ser cuando accede a un sistema o a un servicio.
- f) **Bases de datos:** Colección de información, generalmente relacionada y organizada de manera que se puede acceder, administrar, actualizar y buscar.
- g) **Centro de Procesamiento de Datos:** Área donde reside la infraestructura tecnológica que garantiza la continuidad de los sistemas y servicios de tecnología de la información.
- h) **Certificado autofirmado:** Es un documento digital generado directamente por el firmante o signatario, sin la intervención de una entidad certificadora autorizada, que vincula unos datos de verificación de firma a un signatario y confirma su identidad.
- i) **Copia de respaldo:** También conocida como backup, es la copia que se realiza de la información, con el fin de disponer de un medio para recuperarlos en caso de requerir.
- j) **Cifrado:** Conversión de datos de un formato legible a un formato codificado. Los datos cifrados solo se pueden leer o procesar luego de descifrarlos.
- k) **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a personas o procesos no autorizados.
- l) **Credenciales de acceso:** Nombre de usuario y contraseña que dan acceso a sistemas o servicios.
- m) **Criptografía:** Técnicas de cifrado destinadas a alterar los mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//8. R.D. N° 122/2023

- n) **Cuenta de usuario:** Es un identificador único que se asigna a un usuario del BCB para que a través de una credencial pueda acceder a un sistema o servicio.
- o) **Custodio del activo de información:** Usuario del BCB a quien se le asigna el activo de información y es el encargado directo de hacer efectivos los controles de seguridad definidos por el responsable del activo de información.
- p) **Disponibilidad:** Propiedad de la información de ser accesible y utilizable para los usuarios autorizados.
- q) **Dispositivo móvil:** Dispositivo informático de peso y tamaño reducido, fácilmente transportable y que puede realizar funciones de un equipo computador, tales como laptops, tabletas y teléfonos inteligentes.
- r) **Enmascaramiento de datos:** Técnica de seguridad de sustitución de los datos reales por datos ficticios.
- s) **Etiqueta del activo de información:** Identificador del tipo de clasificación que se le da al activo de información.
- t) **Evento de seguridad de la información:** Ocurrencia identificada en un activo de información que indica una posible infracción de la política de seguridad de la información o falla de controles.
- u) **Incidente de seguridad de la información:** Evento o serie de eventos de seguridad de la información que compromete la seguridad de la información.
- v) **Información confidencial:** Información sobre asuntos y operaciones del BCB, de las instituciones financieras y de sus operaciones, así como de los documentos o informes relacionados con éstas, en el marco de lo establecido en la Ley N° 1670 del BCB en lo concerniente a la confidencialidad.
- w) **Información de uso interno:** Información generada por las Áreas que desarrollan en el nivel operativo actividades especializadas que no se encuentran en el nivel confidencial.
- x) **Información pública:** Información disponible para cualquier persona dentro o fuera del BCB, como ser las publicaciones periódicas.
- y) **Infraestructura de TIC:** Conjunto de hardware, software, redes de comunicación y otros, así como el sitio y recinto que los soporta, que es establecido para el funcionamiento de los sistemas de información, servicios y sistemas de seguridad electrónica.
- z) **Integridad:** Propiedad que salvaguarda la exactitud y completitud de la información.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//9. R.D. N° 122/2023

- aa) **Lineamientos sobre Centro de Procesamiento de Datos:** Lineamiento de la AGETIC denominado “Lineamientos y buenas prácticas para la implementación de un Centro de Procesamiento de Datos”.
- bb) **Lineamientos sobre Seguridad de la Información:** Lineamiento de la AGETIC denominado “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades públicas”.
- cc) **Lineamientos sobre Contingencias Tecnológicas:** Lineamiento de la AGETIC denominado “Lineamientos para la elaboración e implementación de Planes de Contingencia tecnológica en entidades del sector público”.
- dd) **Medio de Almacenamiento Removible:** Es un dispositivo que permite almacenar información y que puede ser extraído fácilmente sin que implique apagar el equipo. Los medios de almacenamiento removibles incluyen discos duros externos, CDs, DVDs y unidades de memoria externa (USB, SD, microSD).
- ee) **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 el BCB.
- ff) **Parche de seguridad:** Conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos.
- gg) **Rack de comunicaciones:** Armario metálico que soporta los equipos informáticos, equipamiento eléctrico y el de comunicaciones.
- hh) **Recinto:** Espacio donde se encuentra ubicado un activo de información.
- ii) **Recinto de comunicaciones y energía eléctrica:** Áreas donde se ubican los racks de comunicaciones y el sistema de energía eléctrica regulada del BCB.
- jj) **Recinto de Archivos:** Áreas donde se almacena documentación en físico del BCB;
- kk) **Recinto de monitoreo:** Áreas donde se realizan las actividades de monitoreo de seguridad electrónica y video vigilancia.
- ll) **Recinto de Tesorería:** Áreas donde se desempeñan operaciones destinadas al manejo del material monetario y valores en custodia.
- mm) **Recintos de copias de respaldo:** Áreas donde se resguardan copias de respaldo de información de seguridad electrónica, sistemas de información y servicios.
- nn) **Recintos de operación de sistema crítico:** Área donde se opera el sistema SWIFT.
- oo) **Responsable del activo de información:** Es la MAA que tiene la atribución de establecer los controles, políticas y directrices de seguridad al activo de información enmarcado al proceso del cual es responsable.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//10. R.D. N° 122/2023

- pp) **Riesgo de seguridad de la información:** Probabilidad de que una amenaza aproveche vulnerabilidades de un activo de información y provoque impacto.
- qq) **Servicio de red:** Llamado también servicio, conjunto de equipos y software conectados entre sí para enviar o recibir información y que permiten implementar servicios tecnológicos (internet, correo electrónico, impresión en red, compartir recursos y otros).
- rr) **Seguridad de la información:** Protección de los activos de información frente a las amenazas que puedan afectar a su confidencialidad, integridad o disponibilidad.
- ss) **Seguridad electrónica:** Equipamiento encargado del control y monitoreo de los sistemas de intrusión física, sensores, alarmas, control de accesos y sistemas de video vigilancia de áreas seguras y otras instalaciones que almacenan información del BCB.
- tt) **Sistema de Información:** Conjunto de componentes interrelacionados que trabajan juntos para recopilar, procesar, almacenar, difundir información y apoyan las operaciones y la toma de decisiones del BCB.
- uu) **Usuario:** Servidora o servidor público, así como consultores y otros que hagan uso de los activos de información del BCB.
- vv) **Vulnerabilidad:** Debilidad de un activo de información o control de seguridad que puede ser aprovechada por una amenaza.

Artículo 5. (Incumplimiento)

El incumplimiento al presente Reglamento será procesado y/o sancionado en el marco del Reglamento Interno de Personal del BCB y de la normativa vigente.

Artículo 6. (Acuerdo de confidencialidad)

A objeto de prevenir fugas de información, divulgación no autorizada o mal uso de la información, se deberá cumplir lo siguiente:

- a) Todo servidor público del BCB debe firmar, una vez al año, un acuerdo o compromiso de confidencialidad gestionado por la Gerencia de Recursos Humanos.
- b) En el caso de contrataciones que realiza el BCB cuando se acceda a los activos de información, las Áreas o Unidades solicitantes deben incorporar un acápite de confidencialidad en los Términos de Referencia o Especificaciones Técnicas.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//11. R.D. N° 122/2023

- c) Los convenios, acuerdos y contratos deben incluir un acápite de confidencialidad cuando se acceda a activos de información del BCB con personas naturales o jurídicas externas.

CAPÍTULO II GESTIÓN DE ACTIVOS DE INFORMACIÓN

Artículo 7. (Activos de Información)

- I. El RSI, en coordinación con las áreas y unidades organizacionales del BCB, elaborará y mantendrá el inventario actualizado de los activos de información.
- II. Los activos de información serán clasificados por los Responsables de Activos de Información del BCB en coordinación con el RSI, dentro de uno de los siguientes niveles:
 - a) Confidencial.
 - b) De uso interno.
 - c) Pública.
- III. La MAA asumirá el rol de responsable del activo de información, de acuerdo a sus atribuciones, quien determinará o identificará al custodio del activo de información al momento de formalizar el inventario.
- IV. Todos los usuarios del BCB se constituirán en custodios de los activos de información asignados, teniendo la obligación de reportar cualquier evento de seguridad de la información que afecte a los mismos.
- V. El Responsable del Activo de información en coordinación con el RSI debe documentar el proceso de asignación y devolución de activos de información a responsables y/o custodios.
- VI. Los activos de información serán etiquetados por el Responsable del Activo de Información en coordinación con el RSI en la matriz de inventario considerando el nivel de clasificación.
- VII. El RSI, en coordinación con las áreas y unidades organizacionales del BCB, establecerá un proceso de manejo, procesamiento, almacenamiento, transmisión, clasificación, desclasificación de los activos de información para cada nivel de clasificación.





BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//12. R.D. N° 122/2023

Artículo 8. (Gestión de medios de almacenamiento removibles)

- I. Los medios de almacenamiento removibles deben ser gestionados por la GSIS para lo cual deberá:
 - a) Gestionar la autorización, uso y retiro de medios de almacenamiento removibles del BCB.
 - b) Mantener un registro de auditoria del uso de medios de almacenamiento removibles. El RSI deberá efectuar el seguimiento.
 - c) Asegurar que el contenido de los medios de almacenamiento removibles que ya no se requieran sean eliminados de manera segura.
- II. El uso de medios de almacenamiento removibles será autorizado solo a usuarios del BCB y provisto por la GSIS a solicitud de la MAA.
- III. La GSIS debe implementar herramientas que permitan cifrar el contenido o permitir el acceso mediante contraseña u otro mecanismo de seguridad para proteger el acceso y el contenido de medios de almacenamiento removibles.
- IV. Es responsabilidad de los usuarios del BCB, aplicar medidas para proteger la información transportada en medios de almacenamiento removibles asignados, evitando accesos no autorizados, daños, pérdida o extravío.

Artículo 9. (Parches de seguridad, actualización de software y gestión de cambios)

Es responsabilidad de la GSIS y la SGR:

- a) Establecer lineamientos de gestión de parches de seguridad y actualización del software.
- b) Planificar y documentar los cambios, bajo ambiente controlado, en sistemas, servicios, infraestructura de TIC y sistemas de seguridad electrónica, asegurando la recuperación ante cambios fallidos e imprevistos.
- c) Establecer criterios para implementar cambios de emergencia en sistemas, servicios, infraestructura de TIC y sistemas de seguridad electrónica.
- d) Establecer líneas base de configuraciones de la infraestructura de TIC y sistemas de seguridad electrónica, que permitan llevar la trazabilidad de los cambios.





BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//13. R.D. N° 122/2023

Artículo 10. (Copia de respaldo y resguardo de información)

Es responsabilidad de la GSIS y la SGR establecer lineamientos de gestión de copias de respaldo y resguardo de la información digital y seguridad electrónica del BCB, que contemplen mínimamente:

- a) Respalidar diariamente toda la información de las operaciones de los sistemas, y bases de datos del BCB para recuperación en casos de contingencia y mensualmente para custodia histórica.
- b) Al menos 2 veces al año respaldar la información organizada en la carpeta D:\BCB de los equipos de los usuarios del BCB, de acuerdo a procedimiento.
- c) Realizar pruebas de restauración de copias de respaldo al menos 1 vez al año de sistemas críticos.
- d) Preservar las copias de respaldo almacenada en cintas u otros medios físicos previendo la renovación de dichos medios por obsolescencia tecnológica.

Artículo 11. (Gestión de vulnerabilidades de los activos de información)

Es responsabilidad de la GSIS y el RSI establecer lineamientos de gestión de vulnerabilidades técnicas y efectuar al menos una vez al año la revisión de vulnerabilidades de los sistemas críticos, que permitan identificar la exposición a las mismas y adoptar acciones preventivas y/o correctivas.

CAPÍTULO III SEGURIDAD FÍSICA Y AMBIENTAL

Artículo 12. (Áreas seguras del BCB)

Se identifican las siguientes áreas seguras en el BCB, con el objeto de prevenir el acceso físico no autorizado e implementar medidas de protección física:

- a) Centros de Procesamiento de Datos.
- b) Recintos de comunicaciones y energía.
- c) Recintos de archivo, ubicados en el Archivo Intermedio y el Archivo Central.
- d) Recintos de monitoreo.
- e) Recintos de Tesorería.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//14. R.D. N° 122/2023

- f) Recintos de copias de respaldo.
- g) Recintos de operación de sistema críticos.

Artículo 13. (Medidas de protección en áreas seguras)

Se establece las siguientes medidas de seguridad en las áreas seguras del BCB, a cargo de la SGR:

- a) Se debe contar con un mecanismo de identificación y autenticación en el ingreso y salida que permita la trazabilidad de los accesos.
- b) El acceso es permitido solo con autorización expresa de la MAA responsable del área segura.
- c) Se debe contar con mecanismos para aplicar controles de seguridad física de áreas e instalaciones seguras, considerando los “Lineamientos sobre Seguridad de la Información”.
- d) Se debe contar con medidas adicionales de seguridad física determinadas a través del análisis de riesgos de seguridad de la información en base a la metodología establecida en el Plan Institucional de Seguridad de la Información del BCB.

Artículo 14. (Trabajo en áreas seguras)

Es responsabilidad de la SGR y las áreas responsables gestionar las actividades dentro de las áreas seguras:

- a) No está permitido el ingreso y trabajo no supervisado de terceras personas y/o servidores públicos ajenos al área.
- b) Es obligatorio portar la identificación de visitante en lugar visible.
- c) Se prohíbe la entrada de equipos de video, fotografía o grabación, de acuerdo a procedimiento.
- d) Las actividades desarrolladas en el área deberán estar monitorizadas por el sistema de video vigilancia.
- e) Debe contar con señalética visible para evacuaciones o contingencias.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//15. R.D. N° 122/2023

Artículo 15. (Medidas de Seguridad de los CPD)

Los Centros de Procesamiento de Datos del BCB deben cumplir los estándares de disponibilidad, redundancia y seguridad de acuerdo a los “Lineamientos sobre Centros de Procesamiento de Datos”.

CAPÍTULO IV CONTROL DE ACCESOS

Artículo 16. (Gestión de credenciales de acceso a sistemas y servicios)

- I. Todo usuario para acceso a sistemas de información o servicios debe utilizar un mecanismo de autenticación conformada por credenciales de acceso, autorizado por la MAA.
- II. La gestión de las credenciales de acceso a los sistemas del BCB debe estar establecida a cargo de la GSIS y la SGR.
- III. La gestión de las credenciales de acceso a los sistemas provistos por terceros implantados en el BCB debe ser establecido por el Área Responsable del Sistema en coordinación con la GSIS.
- IV. Las credenciales de acceso a sistemas y servicios asignados son personales e intransferibles.
- V. Los usuarios del BCB son responsables de la actividad asociada a su cuenta de usuario asignado.
- VI. La GSIS debe proceder con el retiro o bloqueo de las credenciales de acceso otorgados para acceso a sistemas o servicios cuando:
 - a) La Gerencia de Recursos Humanos comunique la vacación, transferencia, rotación, promoción, retiro o cualquier otra modalidad que genere una cesación de funciones o tareas temporales o definitivas de los servidores públicos del BCB.
 - b) La MAA comunique la terminación del contrato o servicio de consultores y otro personal en contrato.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//16. R.D. N° 122/2023

- VII. En caso de desvinculación del servidor público o terminación de contrato, la GSIS debe efectuar la copia de respaldo de la información del equipo de computación asignado.

Artículo 17. (Seguridad de contraseñas)

- I. Los usuarios del BCB son responsables de gestionar de manera segura las contraseñas asignadas.
- II. La GSIS debe establecer las características específicas de las contraseñas que garanticen su confidencialidad y fortaleza.

Artículo 18. (Acceso a los servicios de red)

Todos los accesos a los servicios de red deben estar autorizados por la GSIS en coordinación con las Máximas Autoridades de las Áreas.

Artículo 19. (Acceso a bases de datos y/o equipos servidores)

- I. Los servidores públicos que administran las bases de datos y equipos servidores del BCB, deben estar identificados a través de credenciales de acceso autorizados por una MAA y gestionados por la GSIS.
- II. Todos los accesos a bases de datos en producción deben ser monitoreados y revisados mensualmente por la GSIS.
- III. El RSI deberá efectuar seguimiento al cumplimiento del monitoreo de accesos.

Artículo 20. (Seguridad de dispositivos móviles del BCB)

Es responsabilidad de la GSIS:

- a) Administrar los dispositivos móviles propios del BCB.
- b) Establecer medidas de seguridad para los dispositivos móviles del BCB.





BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//17. R.D. N° 122/2023

Artículo 21. (Dispositivos móviles de los usuarios del BCB)

La GSIS y el RSI deben establecer las condiciones y requisitos de seguridad de los dispositivos móviles de propiedad de los usuarios del BCB para acceso a los recursos del BCB.

CAPÍTULO V DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Artículo 22. (Sistemas de Información)

- I. La GSIS es responsable del desarrollo, mantenimiento e implementación de sistemas de información considerando la confidencialidad, integridad, disponibilidad.
- II. La puesta en producción y la baja de un sistema de información debe ser gestionada por la GSIS en coordinación con las áreas del BCB.

Artículo 23. (Protección de código fuente)

- I. La GSIS debe establecer controles para la protección y copia de respaldo del código fuente de los sistemas de información desarrollados en el BCB, con el objetivo de garantizar la disponibilidad e integridad del mismo y prevenir cambios no autorizados.
- II. La GSIS debe realizar copias de respaldo del código fuente de los sistemas de información al menos una (1) vez al mes.

Artículo 24. (Verificación de los sistemas de información)

- I. Los sistemas de información desarrollados en el BCB deben someterse a una verificación de funcionalidad y requisitos de seguridad de la información establecidos por la GSIS antes de su puesta en producción.
- II. La GSIS para utilizar información de bases de datos de producción en los ambientes de desarrollo o pruebas, aplicará el proceso de enmascaramiento de información, en función al requerimiento de la MAA.

Artículo 25. (Ambientes de desarrollo, prueba y producción)

- I. La GSIS debe implementar controles que garanticen la separación de los ambientes de desarrollo, prueba y producción.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//18. R.D. N° 122/2023

- II. El ambiente de pruebas debe estar configurado con las mismas características de seguridad que el ambiente de producción.

Artículo 26. (Desarrollo de sistemas por consultoría)

Los términos de referencia para el desarrollo de sistemas por consultoría deben contemplar mínimamente lo siguiente:

- a) Cesión de derechos de autor y propiedad intelectual a favor del BCB, sobre el código fuente desarrollado, su contenido o funcionalidad.
- b) Manuales de usuario, manuales técnicos y código fuente.
- c) Requisitos de seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad.

CAPÍTULO VI CORREO ELECTRÓNICO INSTITUCIONAL

Artículo 27. (Gestión del correo electrónico Institucional)

Es responsabilidad de la GSIS:

- a) Establecer las características técnicas del Correo Electrónico Institucional.
- b) Asignar una cuenta de correo institucional grupal a las áreas solicitantes de acuerdo a evaluación técnica.
- c) Implementar herramientas para la protección del correo institucional.
- d) Otorgar el acceso al contenido del buzón de una cuenta de correo electrónico a requerimiento de una MAA.

Artículo 28. (Uso del correo electrónico Institucional)

Los usuarios del BCB deben cumplir lo siguiente:

- a) Usar la cuenta de correo electrónico institucional únicamente para fines laborales y de carácter institucional.
- b) Mantener la confidencialidad, reserva del envío y recepción de información.





BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//19. R.D. N° 122/2023

CAPÍTULO VII USO DE CRIPTOGRAFÍA

Artículo 29. (Controles criptográficos)

La GSIS debe establecer controles criptográficos para la protección, transmisión y el resguardo de información, de acuerdo a los “Lineamientos sobre Seguridad de la Información”.

CAPÍTULO VIII SEGURIDAD EN EL TELETRABAJO

Artículo 30. (Condiciones de acceso remoto para teletrabajo)

- I. La GSIS y el RSI deben establecer las condiciones técnicas y de gestión de acceso remoto para teletrabajo.
- II. Durante el teletrabajo, es responsabilidad del usuario del BCB, conservar y custodiar con la debida diligencia la información en físico y digital.

CAPÍTULO IX SEGURIDAD DE LAS COMUNICACIONES Y SERVICIOS DE RED

Artículo 31. (Seguridad en redes)

Es responsabilidad de la GSIS:

- a. Proteger la información que se transmiten a través de la red de telecomunicaciones externas o internas, mediante técnicas de cifrado estándar a través de equipos o aplicaciones de acuerdo a los “Lineamientos sobre Seguridad de la Información”.
- b. Establecer los requisitos de seguridad para el acceso a la red del BCB por parte de participantes externos.



BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//20. R.D. N° 122/2023

Artículo 32. (Monitoreo de los servicios de red)

La GSIS debe establecer las herramientas necesarias para realizar el monitoreo de la disponibilidad de los servicios de red.

Artículo 33. (Uso adecuado de los servicios de red)

- I. La GSIS debe establecer las condiciones de uso del servicio de Internet por parte de los usuarios del BCB.
- II. Los usuarios del BCB son responsables del uso y el contenido en texto, audio o imágenes que emita o envíe a través de los servicios de red precautelando la confidencialidad y la imagen institucional.
- III. Está restringido el acceso a redes sociales, servicios de correo electrónico gratuitos, servicios de mensajería instantánea, servicios de medios tipo “streaming” y servicios de almacenamiento externo desde los computadores y portátiles del BCB, salvo autorización expresa de la MAA.

CAPÍTULO X

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Artículo 34. (Gestión de incidentes de seguridad de la información)

- I. El RSI debe establecer la gestión de incidentes de seguridad de la información, manteniendo un registro que permita adoptar medidas de control para prevenir, detectar, gestionar, reportar y resolver.
- II. La GSIS debe contar con un Plan de Contingencias Tecnológicas, para la continuidad de los sistemas y servicios de tecnología de la información y comunicación, actualizado e implementado considerando los “Lineamientos sobre Contingencias Tecnológicas”





BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//21. R.D. N° 122/2023

CAPÍTULO XI **OBLIGACIONES SOBRE SEGURIDAD DE LA INFORMACIÓN**

Artículo 35. (Obligaciones)

Los usuarios del BCB tienen la obligación de:

- a) Bloquear la sesión del equipo de computación al ausentarse del puesto de trabajo.
- b) No publicar ni compartir las contraseñas de los sistemas y servicios del BCB.
- c) Aceptar y cumplir el acuerdo de confidencialidad.
- d) Reportar incidentes que afecten la confidencialidad, integridad y disponibilidad de un activo de información a su cargo.
- e) Dejar los escritorios o mesas de trabajo despejados de documentación y de medios de almacenamiento removibles.
- f) No destruir o eliminar o borrar información confidencial y/o de uso interno del BCB.
- g) No alterar la configuración del equipo de computación asignado e instalar aplicaciones o software no autorizadas.
- h) No utilizar software de hacking u otros sin autorización que atenten contra la información e infraestructura de TIC del BCB.

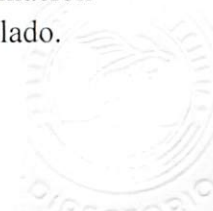
CAPÍTULO XII **SEGURIDAD DE LA INFORMACIÓN EN FÍSICO**

Artículo 36. (Criterio de Archivo)

El archivo de los documentos en físico debe realizarse de acuerdo con los criterios previstos en el Reglamento de Gestión Documental del BCB debiendo garantizar la correcta conservación de los documentos, la localización y consulta de la información.

Artículo 37. (Medidas de protección para información en físico)

Las medidas de protección para la información en físico deben aplicar a información clasificada como confidencial o de uso interno en la reproducción, el acceso y el traslado.





BANCO
CENTRAL DE
BOLIVIA



ESTADO PLURINACIONAL DE
BOLIVIA

DIRECTORIO

//22. R.D. N° 122/2023

DISPOSICIÓN FINAL

Disposición final única

En el marco de la normativa emitida por el Órgano Rector del Sistema Nacional de Tesorería y Crédito Público con relación al Sistema de Pagos del Tesoro, el uso de certificados autofirmados es válido y se encuentra circunscrito únicamente a la seguridad informática, para lo cual la GSIS gestionará las claves de certificado autofirmado en coordinación con el área correspondiente.

