Resolución del
Consejo de Administración
N° 70/2021

TEMA: **APROBACION DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA FUNDACIÓN CULTURAL DEL BANCO CENTRAL DE BOLIVIA**

VISTOS:

La Constitución Política del Estado.

La Ley Nº 1670, de 31 de octubre de 1995, del Banco Central de Bolivia.

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

La Ley N° 398, de 02 de septiembre de 2013.

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 09 de septiembre de 2015, crea la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación ACETIC

La Resolución Administrativa AGETIC/RA/0051/2017 de fecha 19 de septiembre de 2017, a través de la cual se aprueban los Lineamientos para la Elaboración de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Púbico

El Estatuto de la Fundación Cultural del Banco Central de Bolivia, aprobado por el Directorio del Banco Central de Bolivia mediante Resolución N° 052/2018 de 17 de abril de 2018.

El Informe Técnico FCBCB/UNAF/SIS/INF N°040/2021, de 23 de julio de 2021, la Comisión de Equipo Técnico de la Elaboración del Plan Institucional de Seguridad de la Información de la Fundación Cultural del Banco Central de Bolivia.

El Informe Técnico FCBCB – DG N° 24/2021, de 29 de julio de 2021, de la Sección Organizacional de Planificación.

El Informe FCBCB/UNAF/SIS/INF N° 048/2021, de 13 agosto de 2021, los Miembros del Comité de Seguridad de la Información de la Fundación Cultural del Banco Central de Bolivia.

El Informe FC BCB-UNAJ N° 247/2021, de 16 de agosto de 2021, de la Unidad Nacional de Asuntos Jurídicos.

El Acta N°36, de fecha 19 de agosto de 2021, del Consejo de Administración de la Fundación Cultural del Banco Central de Bolivia.

CONSIDERANDO:

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

Que la Ley N° 164, de 8 de agosto de 2011, General de Telecomunicaciones Tecnologías de Información y Comunicación, en su Artículo 71 declara prioridad nacional la promoción del uso de tecnologías; asimismo, dispone 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

Calle Fernando Guachalla Nº 476
Telfs: 2424148 - 2418419 | Casilla postal 12164
E-mail: fundacion@fundacionculturalbcb.gob.bo | www.fundacionculturalbcb.gob.bo
La Paz - Bolivia

seguridad informática y de 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; al efecto establece en el Parágrafo I del Artículo 75, que el nivel central del Estado promueva la incorporación del Gobierno Electrónico a los procedimientos gubernamentales, a la prestación de sus servicios y a la difusión de información, mediante una estrategia enfocada al servicio de la población. Asimismo, establece que el órgano Ejecutivo del nivel central del Estado, elaborará los lineamientos para la incorporación del Gobierno Electrónico.

Que Decreto Supremo N° 1793, de 13 de noviembre de 2013, que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, establece: los principios para el desarrollo y uso de aplicaciones informáticas en las entidades públicas; los objetivos del Gobierno Electrónico; y que las entidades públicas del estado, estarán a cargo de la Ejecución de la Implementación del Gobierno Electrónico. De la misma forma en el 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 involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad. De la misma forma, el inciso d) Parágrafo II del Artículo 4, en cuanto al tratamiento de datos personales, determina que se deben 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.

De acuerdo con el Artículo 8 del mismo Reglamento, arriba mencionado, dispone 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 Decreto Supremo N° 2514, de 9 de septiembre de 2015, crea la Agencia de Gobierno Electrónico y Tecnologías y Comunicación (AGETIC) y los Comités Interinstitucionales de Simplificación de Trámites; estableciendo en los incisos f) e i) del Artículo 7, entre sus funciones; Establecer los lineamientos técnicos en seguridad de la información para las entidades del sector público y elaborar, proponer, promover, gestionar, articular y actualizar planes relacionados con la seguridad informática. De la misma forma, 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). Cuyo Plan Institucional, de acuerdo a la Disposición Transitoria Segunda del citado Decreto Supremo, deberá ser presentado a la Agencia de Gobierno Electrónico y Tecnologías de la información y Comunicación (AGETIC9, en un plazo no mayor a un (1) año, desde la aprobación de las políticas de seguridad de la información por la AGETIC.

La Resolución Administrativa AGETIC/RA/0051/2017, de 18 de septiembre de 2017, del Pleno del Concejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia - CETIC-EPB, que aprobó los "Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", conforme lo dispone el inciso f) del Artículo 7 del Decreto Supremo N° 2514, de 9 de septiembre de 2015.

Los "Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", establecen que, para la implementación del referido Plan, la Máxima Autoridad Ejecutiva de la entidad en una etapa inicial debe designar al Responsable de Seguridad de Información y conformar el Comité de Seguridad de la Información.

Que el sub numeral 6.1.1, del documento de "Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", aprobados por la Resolución Administrativa AGETIC/RA/0051/2017, de 18 de septiembre de 2017, establecen que, son responsabilidades de la Máxima Autoridad Ejecutiva (MAE) respecto a la

Calle Fernando Guachalla N° 476
Telfs: 2424148 - 2418419 | Casilla postal 12164
E-mail: fundacion@fundacionculturalbcb.gob.bo | www.fundacionculturalbcb.gob.bo
La Paz - Bolivia

seguridad de la Información, que deberá: a) Estar informada sobre el estado de seguridad de la información de la entidad o institución pública bajo su tutela; b) Tomar conocimiento de la normativa vigente respecto a seguridad de la información (Decreto Supremo N° 2514, de 9 de septiembre de 2015 y Decreto Supremo N° 1793, de 13 de noviembre de 2013, de reglamentación general a la Ley N° 164, aprobada mediante Decreto supremo N° 1391, de 8 de agosto de 2011; c) Designar al Responsable de Seguridad de la Información (RSI); d) Conformar el Comité de Seguridad de la Información; e) Asegurar que los objetivos y alcances del Plan Institucional de Seguridad de la Información sean compatibles con los objetivos del Plan Estratégico Institucional; f) En lo posible, destinar los recursos administrativos, económicos y humanos para la elaboración e implementación del Plan Institucional de Seguridad de la Información; g) Aprobar el Plan Institucional de Seguridad de la Información de su entidad o institución; h) Cumplir y hacer cumplir el Plan Institucional de Seguridad de la Información de su entidad o institución.

Que el punto 6.1.3, del documento arriba referido los "Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", establece sobre la Conformación y Funciones del Comité de Seguridad de la Información que, "*El CSI establecerá su organización interna y asumirá como mínimo las siguientes funciones: a) Revisar el Plan Institucional de Seguridad de la Información (PISI); b) Promover la aprobación del PISI a través de la MAE; (…).*

CONSIDERANDO:

Que el Artículo 81 de la Ley N° 1670, de 31 de octubre de 1995, del Banco Central de Bolivia, crea a la Fundación Cultural del Banco Central de Bolivia con el objeto de mantener, proteger, conservar, promocionar y administrar los Repositorios Nacionales que se encuentran bajo su tuición, administración y dependencia.

Que el Artículo 2 de la Ley Nº 398 de 03 de septiembre de 2013, que modifica el artículo 82 de la Ley Nº 1670, establece que: *"La Fundación tendrá la tuición administrativa de los siguientes repositorios nacionales: Casa Nacional de la Moneda (Potosí), Casa de la Libertad (Sucre), Archivo y Biblioteca Nacionales de Bolivia (Sucre), Museo Nacional de Etnografía y Folklore (La Paz), Museo de Arte (La Paz) y el Centro de la Cultura Plurinacional (Santa Cruz), sin que pierdan su condición de patrimonio cultural e histórico del Estado Plurinacional".* Asimismo, la Fundación Cultural del Banco Central de Bolivia tiene bajo su tuición y administración al Centro Cultural de reciente creación: Centro de la Revolución Cultural, creado mediante Resolución de Directorio N° 098/2018, de 31 de julio de 2018, del Banco Central de Bolivia.

Que el Artículo 9 del Estatuto de la Fundación Cultural del Banco Central de Bolivia, aprobado por el Directorio del Banco Central de Bolivia, mediante Resolución N° 052/2018, de 17 de abril de 2018, establece que la Máxima Autoridad de la Fundación Cultural del Banco Central de Bolivia, es su Consejo de Administración, responsable de definir políticas de esta institución, establece sus estrategias administrativas, financieras, operativas y su normativa interna, con la finalidad de procurar el cumplimiento de su objeto.

Que de acuerdo al Artículo 10, Inciso: a), del Estatuto de la Fundación Cultural del Banco Central de Bolivia, el Consejo de Administración tiene la atribución de: *"Formular políticas y estrategias institucionales, así como realizar seguimiento a su implantación."*

Que el Artículo 15 del Estatuto de la Fundación Cultural del Banco Central de Bolivia, señala que el Presidente del Consejo de Administración es responsable por la gestión y administración institucional de la Fundación, que tiene entre sus atribuciones: *"a) Cumplir y hacer cumplir las Políticas*

VoBo PRESIDENCIA L.C.O. La Paz-Bolivia

VoBo

ELABORADO POR: Abog. Erika Habe Gómez RESPONSABLE DE ANÁLISIS JURÍDICO a.i.

Institucionales, el Estatuto, las decisiones adoptadas por el Consejo de Administración y el ordenamiento jurídico aplicable, dentro de los alcances del objeto de la FCBCB".

Que Informe Técnico FCBCB/UNAF/SIS/INF N°040/2021, de 23 de julio de 2021, la Comisión de Equipo Técnico de la Elaboración del Plan Institucional de Seguridad de la Información de la Fundación Cultural del Banco Central de Bolivia, a partir de la instrucción encomendada por la Dirección General, actualizó el Cronograma Implementación y el Plan de Seguridad de la Información de la Fundación Cultural de Banco Central de Bolivia, a ser ejecutado desde agosto de 2021 hasta agosto de 2022, en el marco del Informe Técnico FCBCB/UNAF/SI_INF/N° 008/2019, de 03 de junio de 2019 y el documento anexo del Plan Institucional de Seguridad de la Información (P.I.S.I.) Versión 1.01.

Que el Informe Técnico FCBCB – DG N° 24/2021, 29 de julio de 2021, del Profesional de Gestión Institucional a.i. y la Responsable de Planificación a.i., señala respecto del Plan Institucional de Seguridad de la Información (P.I.S.I.) de la FCBCB, en conclusiones establecen que el objetivo del Plan Institucional de Seguridad de la Información (P.I.S.I.) de la FC-BCB se encuentra alineado a la planificación estatal en materia de información y comunicación, así como a la planificación estratégica y operativa de la FC-BCB; se articula a la Acción de Mediano Plazo 4 del Plan Estratégico Institucional (PEI) 2016 – 2020 de la entidad, la cual se encuentra vinculada a la gestión técnica que garantice la eficiencia de todos los procesos desarrollados por la institución el documento se realizó en base a los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público, que fueron emitidos por la AGETIC y da cumplimiento a la normativa legal vigente.

Que mediante Informe FCBCB/UNAF/SIS/INF N°048/2021, de 13 de agosto de 2021, emitido por los Miembros del Comité de Seguridad de la Información de la Fundación Cultural del Banco Central de Bolivia, establecen los objetivos e importancia del Plan Institucional de Seguridad de la Información P.I.S.I., luego de la revisión del documento presentado, establece en conclusiones que: *"El Plan de Implementación de Seguridad de la información cumple con los requerimientos y se elaboró de acuerdo a la información pertinente a la FCBCB; el Plan de Implementación de Seguridad de la información se elaboró con base a los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público, que fueron emitidos por la Agencia de Gobierno Electrónico, Tecnologías de Información y Comunicación (AGETIC) y da cumplimiento a la normativa legal vigente; los informes FCBCB/UNAF/SI_INF/N°008/2019 de fecha 3 de junio de 2019 y FCBCB — DG N° 24/2021, 29 de julio de 2021 señalan que el P.I.S.I. fue elaborado de acuerdo a normativa vigente y recomiendan su aprobación al Consejo de Administración solicitando los informes correspondientes bajo normativa vigente; el análisis y evaluación en seguridad de la información es un proceso dinámico que debe gestionarse constantemente, los resultados podrían variar de un intervalo de tiempo a otro por nuevas amenazas identificadas y/o debido a los controles implementados."* En este contexto, recomienda: "*Remitir el presente pronunciamiento a la Unidad de Asuntos Jurídicos para la emisión del Informe Legal respectivo y poner a consideración del Consejo de Administración de la FC-BCB, la aprobación del Plan de Implementación de Seguridad de la Información de la Fundación Cultural del Banco Central de Bolivia mediante resolución expresa*".

Que el Informe FC BCB-UNAJ N° 247/2021, de 16 de agosto de 2021, concluye que es viable jurídicamente la aprobación del Plan Institucional de Seguridad de la Información (P.I.S.I.) de la Fundación Cultural del Banco Central de Bolivia, al encontrarse técnicamente justificado por las áreas competentes de la Fundación Cultural del Banco Central de Bolivia, por lo que recomienda la aprobación del Plan Institucional de Seguridad de la Información (P.I.S.I.) de la FC-BCB, por la instancia

Calle Fernando Guachalla Nº 476
Telfs: 2424148 - 2418419 | Casilla postal 12164
E-mail: fundacion@fundacionculturalbcb.gob.bo | www.fundacionculturalbcb.gob.bo
La Paz - Bolivia

pertinente, así como se instruya que el mismo sea publicado y puesto en conocimiento de las áreas organizacionales de la Fundación Cultural del Banco Central de Bolivia, por la Unidad Nacional de Administración y Finanzas y las Unidades de Administración de los Repositorios Nacionales y Centros Culturales; por otra parte, se debe remitir a la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación AGETIC, el P.I.S.I. y la documentación pertinente de acuerdo a la normativa vigente.

Que se instruye la elaboración de la presente Resolución en Consejo de Administración de la Fundación Cultural del Banco Central de Bolivia, conforme a Acta N° 36, de fecha 19 de agosto de 2021.

POR TANTO:

El ***CONSEJO DE ADMINISTRACIÓN DE LA FUNDACIÓN CULTURAL DEL BANCO CENTRAL DE BOLIVIA***, en uso de sus específicas funciones y atribuciones,

R E S U E L V E:

PRIMERO.- **APROBAR**, el Informe FCBCB/UNAF/SIS/INF N°048/2021, de 13 de agosto de 2021, emitido por los Miembros del Comité de Seguridad de la Información de la Fundación Cultural del Banco Central de Bolivia, que adjunta el Plan Institucional de Seguridad de la Información (P.I.S.I.) de la FC-BCB; así mismo, el Informe FC BCB-UNAJ N° 247/2021, de 16 de agosto de 2021, de la Unidad Nacional de Asuntos Jurídicos.

SEGUNDO.- **APROBAR,** el Plan Institucional de Seguridad de la Información (P.I.S.I.) de la Fundación Cultural del Banco Central de Bolivia.

TERCERO.- **ENCOMENDAR** a la Unidad Nacional de Administración y Finanzas y las Unidades de Administración de los Repositorios Nacionales y Centros Culturales, la publicación y puesta en conocimiento de las áreas organizacionales de la Fundación Cultural del Banco Central de Bolivia, el Plan Institucional de Seguridad de la Información (P.I.S.I.), en cumplimiento de la presente Resolución.

Regístrese, comuníquese, cúmplase y archívese.

La Paz, 19 agosto de 2021.

Luis Oporto Ordoñez
PRESIDENTE

Jhonny Quino Choque
CONSEJERO

Susana Bejarano Auad
CONSEJERA

José Antonio Rocha Torrico
CONSEJERO

Guido Pablo Arze Mantilla
CONSEJERO

Roberto Aguilar Quisbert
CONSEJERO

Para regularizar por viaje.

VºBº Rolando Espinoza
FUNDACION CULTURAL BANCO CENTRAL DE BOLIVIA
ELABORADO POR: Abog. Erika Hebe Gómez
RESPONSABLE DE ANALISIS JURIDICO a.i.

Calle Fernando Guachalla Nº 476
Telfs: 2424148 - 2418419 | Casilla postal 12164
E-mail: fundacion@fundacionculturalbcb.gob.bo | www.fundacionculturalbcb.gob.bo
La Paz - Bolivia

Fundación Cultural
Banco Central de Bolivia

Plan Institucional de Seguridad de la Información (P.I.S.I.)

Versión 1.01

FUNDACIÓN CULTURAL DEL BANCO CENTRAL DE BOLIVIA
Calle Fernando Guachalla N° 476
www.fundacionculturalbcb.gob.bo

2021

ÍNDICE

1. INTRODUCCIÓN

Hoy por hoy la información se constituye en uno de los activos más valiosos en toda institución; su proceso, almacenamiento y manejo son de interés tanto institucional como estatal, debiendo definirse los lineamientos para su adecuada administración.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de garantizar su confidencialidad, integridad, disponibilidad y privacidad; razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación para el Estado.

El presente Plan busca establecer los lineamientos generales en materia de seguridad de la información de la Fundación Cultural del Banco Central de Bolivia FC-BCB, así como de los Repositorios Nacionales y Centros Culturales bajo su tuición:

- Museo Nacional del Arte (MNA)
- Museo Nacional de Etnografía y Folklore (MUSEF)
- Centro de la Cultura Plurinacional (CCP)
- Archivo y Bibliotecas Nacionales de Bolivia (ABNB)
- Casa Nacional de Moneda (CNM)
- Casa de la Libertad (CDL)
- Centro de la Revolución Cultural (CRC)

La Fundación Cultural del Banco Central de Bolivia, a través de su Máxima Autoridad Ejecutiva, sus Áreas Organizacionales, Unidades Organizacionales y todo el personal dependiente; declara su compromiso irrefutable para la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información, el cual permita establecer los procedimientos y controles para una efectiva protección de activos de información – físicos o digitales – de conformidad a las disposiciones normativas al respecto.

2. MARCO NORMATIVO

La normativa vigente, que respalda la elaboración del presente Plan Institucional de Seguridad de la Información de la FC-BCB, se encuentra compuesto por:

- El Parágrafo I del Artículo N° 72 de la Ley N° 164 de 28 de julio de 2011, Ley General de Telecomunicaciones, que establece 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 de 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*".

  El inciso d) del Artículo N° 4 (Principios), parágrafo II, del Decreto Supremo N° 1793 de 13 de noviembre de 2013, que señala 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".

- El Artículo N° 8 (Plan de contingencia) del Decreto Supremo N° 1793, de 13 de noviembre de 2013, refiere: "*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*".

- El Decreto Supremo N° 2514 de 9 de septiembre de 2015, el cual dispone principalmente que la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) establecerá: "*Los lineamientos técnicos en seguridad de información para las entidades del sector público*". Asimismo, establece como parte de sus funciones "*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*". Por otra parte, norma la creación del "Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC, encargado de "*Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público*".

- El Decreto Supremo N° 3251 del 12 de Julio de 2017 que aprueba el Plan de Implementación de Gobierno Electrónico, estableciendo como una de las líneas estratégicas del mismo, la seguridad informática y de la información, cuya programación debe estar incluida en dicho Plan.

- Resolución Administrativa AGETIC/RA/0051/2017 de fecha 19 de septiembre de 2017, a través de la cual el Consejo para las Tecnologías de la Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB) aprueba el documento "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público".

Bajo este marco, la Fundación Cultural del Banco Central de Bolivia – en cumplimiento a lo establecido en la Política de Seguridad de la Información emanado por la AGETIC – emprende la implementación de una Estrategia de Gestión de Seguridad de la Información, con el objeto de proteger los sistemas y activos de información con lo que cuenta.

Para ello, se efectúa la identificación de activos de información riesgosos y posterior aplicación de controles de seguridad, a fin de mitigar los riesgos que están inherentes en los procesos y actividades de la institución, buscando alcanzar el cumplimiento de la misión y objetivos institucionales desde una perspectiva de la seguridad de la información, aplicando nuevos

controles orientados a la preservación de la confidencialidad, disponibilidad e integridad de la información institucional.

3. DIAGNÓSTICO INSTITUCIONAL

La Fundación Cultural del Banco Central de Bolivia que tiene por finalidad rescatar, proteger, custodiar, conservar, restaurar, promover y poner en valor el patrimonio cultural tangible e intangible que se encuentra en los repositorios, rescatando la historia y cultura.

La FC-BCB fue creada el año 1995, mediante Ley N°1670 e inició sus actividades en 1997, teniendo bajo su tuición – inicialmente – cuatro Repositorios Nacionales: Casa Nacional de Moneda (Potosí); Archivo y Biblioteca Nacionales de Bolivia; Casa de la Libertad (Sucre) y Museo de Etnografía y Folklore (La Paz); a los que – posteriormente – se sumaron el Museo Nacional de Arte (La Paz) el año 2002, el Centro de la Cultural Plurinacional (Santa Cruz de la Sierra) y finalmente el Centro de la Revolución Cultural (La Paz).

La Fundación Cultural del Banco Central de Bolivia durante el proceso de desarrollo de aplicaciones, solo toma en cuenta la funcionalidad de las aplicaciones, más no la protección total de la información que en esta se procesa; dando lugar – potencialmente – a ataques de hackers, espías corporativos y a que la información de las Áreas Organizacionales, típicamente sensible y confidencial se vea afectada en algunas ocasiones.

Se han hecho esfuerzos importantes para protegerse de ataques informáticos, provenientes de internet e incluso de ataques generados por servidores públicos de la propia institución, que por diferentes motivos pueden causar grandes pérdidas, no solo económicas o en cuanto a reputación, sino también en otros aspectos relevantes para las operaciones que desarrolla la entidad.

4. TÉRMINOS, DEFINICIONES Y SIGLAS

En este acápite se presentan los términos, definiciones y siglas como referencia de los términos utilizados a lo largo del documento.

Activo: Son los bienes, derechos y otros recursos de los que dispone una empresa, pudiendo ser, muebles, construcciones, equipos informáticos o derechos de cobro por servicios prestados o venta de bienes.

Activo de Información: En seguridad de la información corresponde a aquellos datos físicos, digitales, sistemas y elementos tanto de hardware como de software que se encuentran relacionados con el flujo o almacenamiento de información, conocimientos o datos que tienen valor para la organización.

Los activos de la información, responden a la siguiente clasificación:

- **Información:** En esta clasificación ingresan procesos relevantes para la institución e información en cualquier medio de soporte físico o digital. Los tipos de información que ingresarían son: información estratégica, información relacionada con el archivo personal, información relacionada a la documentación administrativa, legal, procesos

de adjudicación y otros que tengan un coste económico y de cumplimiento con la normativa legal. También, en esta categoría está la información de archivos tales como respaldos, documentos, credenciales de acceso, entre otros.

- **Claves criptográficas:** Algunos de los ejemplos de activos en esta categoría son: claves para cifrar, firmar, certificados x509, entre otros.
- **Servicios:** En esta categoría ingresan: servicios de acceso remoto, transferencia de archivos, correo electrónico, servicios web, servicio de directorio, entre otros.
- **Software – aplicaciones informáticas:** En esta categoría se encuentran: sistemas desarrollados y/o adquiridos, software de aplicación, sistemas operativos, software de virtualización, entre otros.
- **Equipamiento informático (Hardware):** En esta categoría están los medios físicos que soportan los procesos como ser: servidores, equipamiento de escritorio, periféricos, dispositivos de red perimetral, dispositivos de red, corta fuegos, entre otros.
- **Redes de comunicaciones:** Están los servicios de comunicaciones como ser: la red telefónica, redes de datos, internet, entre otros.
- **Soportes de información:** En esta categoría están: discos virtuales y físicos, memorias usb, discos y cintas, material impreso, entre otros.
- **Equipamiento auxiliar:** En esta categoría están: fuentes de alimentación, generadores eléctricos, equipos de climatización, cableado eléctrico, mobiliario, entre otros.
- **Instalaciones:** Edificio, vehículos, instalaciones de refuerzo, entre otros.
- **Personal:** Incluye personal fijo, eventual, terceros, entre otros. También se debe identificar a los responsables y custodios de la información asociada al activo; esto es importante porque a través de la identificación se realizará una mejor valoración para resguardar la información. Los custodios podrían ser los mismos servidores públicos o en otros casos una persona ajena a la entidad o institución pública.

Clave: Contraseña o password, que permite la autentificación y control del acceso hacia algún recurso.

Confidencial: Se trata de una propiedad de la información que pretende garantizar el acceso solo a personas autorizadas.

Disponibilidad de la información: Es la característica, cualidad o condición de la información, que la hace accesible a quienes deben acceder a ella, ya sean personas, procesos y/o aplicaciones.

Estrategia de Gobierno Electrónico: Estrategia definida por el Gobierno Nacional del Estado Plurinacional de Bolivia que busca apoyar y homologar los contenidos y servicios ofrecidos por cada una de las entidades públicas, para el cumplimiento de los objetivos de un Estado más eficiente, transparente y participativo, que preste servicios a través del aprovechamiento de las tecnologías de información.

Información pública: Es toda aquella información generada, obtenida, adquirida, o controlada que no presenta restricciones para su acceso.

Información pública clasificada: Es aquella información que estando en poder o custodia de un funcionario, pertenece al ámbito propio, particular y privado o semi – privado de una

persona natural o jurídica, por lo que su acceso podrá ser negado, siempre que se trate de circunstancias legítimas y necesarias.

Información pública reservada: Es aquella información que estando en poder o custodia de un funcionario, es negada al acceso a la ciudadanía, por daño a intereses públicos.

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos; incluye virus, gusanos, troyanos y puertas traseras.

Mecanismos de bloqueo: Son los mecanismos necesarios para impedir que los usuarios, de los sistemas de información y de los servicios, tengan acceso a los mismos sin previa autorización, ya sea por razones de seguridad, falta de permisos, intentos malintencionados o solicitud de los propietarios de la información.

Phishing (cosecha y pesca de contraseñas): Es un delito cibernético, en el cual por medio del envío de correos se invita a las personas a que visiten páginas web falsas de entidades bancarias o comerciales.

Política: Declaración general de principios que presenta la posición de la institución para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas.

Seguridad de la información: Propiedad que hace referencia a la disponibilidad de la información, ya sea que esta no pueda ser revelada a individuos no autorizados, entidades o procesos, o ser accesibles y utilizables a la demanda de una entidad autorizada; asimismo se refiere a la integridad y protección de la exactitud de los activos, autenticidad y no repudio, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento de la información.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad se caracteriza por ausencia en controles de seguridad que permite ser explotada.

Ataque: Es la acción de interrumpir o dañar un activo de información con el objetivo de causar problemas de confiabilidad, disponibilidad e integridad; o en su defecto es la materialización de la amenaza.

Código malicioso: Software diseñado para ejecutar acciones maliciosas, como provocar daños al software de la computadora, robar información almacenada en un sistema informático, aprovechar recursos informáticos para efectuar otras acciones perjudiciales para el usuario, entre otros. Este tipo de software incluye programas como virus, gusanos, troyanos y spyware; pudiendo utilizar como vía de diseminación el correo electrónico, sitios de internet, redes, dispositivos móviles y/o dispositivos removibles.

Firewall: Un firewall o también llamados cortafuegos, es un sistema diseñado para prevenir el acceso no autorizado hacia o desde una red privada. Se puede implementar en forma de hardware o en una combinación de ambos. Los cortafuegos impiden que los usuarios no autorizados accedan a redes privadas conectadas a internet, especialmente a intranets.

Confidencialidad: Todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta

después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.

Tecnología de la información: Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y servicios.

Usuario de la información: Es aquella persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos, ya sea generar contenido y documentos, utilizar software de diverso tipo, entre otras.

Copias de Seguridad: Denominada copia de seguridad, respaldo, copia de respaldo, copia de reserva o *backup*, es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Seguridad informática: Es el conjunto de normas, procedimientos y herramientas, que se enfocan en la protección de la infraestructura computacional y la información contenida o circulante.

Plan de contingencia: Es un instrumento que comprende un conjunto de métodos y acciones para el buen gobierno de las tecnologías de la información y comunicación en el dominio del soporte y el desempeño, contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio y las operaciones de una entidad, en circunstancias de riesgo, crisis y otras situaciones anómalas.

Teletrabajo

El teletrabajo es una modalidad de relación laboral o de prestación de servicios, que consiste en el desempeño de actividades remuneradas, utilizando las TIC en el marco de un contrato o de una relación de trabajo, en la cual no se requiere la presencia física del teletrabajador, siempre que las necesidades y naturaleza del trabajo lo permitan.

Emergencia sanitaria

La emergencia sanitaria acaece cuando una o varias enfermedades constituyan un riesgo para la salud pública, implique una situación de extrema gravedad y magnitud que dañe directamente a las personas y provoque una crisis sanitaria, sean éstos por un brote epidémico que afecte o exista contagios comunitarios al interior del territorio nacional o sea declarada como epidemia o pandemia.

CUADRO N° 1
ABREVIACIONES EMPLEADAS EN EL P.I.S.I.

SIGLA	DESCRIPCIÓN
ISO 27001:2015	Norma técnica del comité ISO (Sistema de Gestión de Seguridad de Información)
CSI	Comité de Seguridad de Información
RSIMM	Responsable de Seguridad de Información
BIA	Análisis de Impacto al Negocio
AGETIC	Agencia Gobierno Electrónico y Tecnologías de Información y Comunicación

SIGLA	DESCRIPCIÓN
CTIC-EPB	Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia
CGII	Centro de Gestión de Incidentes Informáticos
PISI	Plan Institucional de Seguridad de Información
PSI	Política de la Seguridad de Información
MAE	Máxima Autoridad Ejecutiva
FC-BCB	Fundación Cultural del Banco Central de Bolivia

Fuente: *Elaboración Propia*

5. OBJETIVOS DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

El objetivo del presente documento, es definir – y consecuentemente implementar – políticas, lineamientos, procedimientos, normativa y controles de seguridad de la información en la Fundación Cultural del Banco Central de Bolivia con base a los lineamientos normativos establecidos, para mitigar los niveles de riesgos, preservando un nivel aceptable en la confidencialidad, integridad y disponibilidad de la información institucional; así como para asegurar el desarrollo, mantenimiento y soporte de sistemas de información que necesita la Fundación, incorporando parámetros necesarios de seguridad de la información en concordancia con la normativa legal vigente del Estado Plurinacional de Bolivia.

6. ALCANCE DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

Las políticas y procedimientos contemplados en el presente Plan Institucional de Seguridad de la Información, serán aplicadas con cumplimiento obligatorio en todas las Áreas Organizacionales dependientes de la FC-BCB, empresas contratistas y terceros que interactúen con la institución.

6.1 Áreas Organizacionales de la FC-BCB

Las Áreas Organizacionales involucradas en el proceso de implementación del plan y que integran en su conjunto, el funcionamiento de los procesos esenciales de la institución es:

- ✓ Consejo de Administración
- ✓ Presidencia
  - Dirección General
  - Unidad Nacional de Administración y Finanzas
  - Unidad Nacional de Asuntos Jurídicos
  - Unidad Nacional de Gestión Cultural
  - Unidad Nacional de Gestión de Infraestructura
- ✓ Museo Nacional de Etnografía y Folklore (MUSEF)
  - Regional MUSEF – Sucre
- ✓ Museo Nacional de Arte (MNA)
- ✓ Casa Nacional de la Moneda (CNM)
- ✓ Archivo y Biblioteca Nacionales de Bolivia (ABNB)
- ✓ Casa de la Libertad (CDL)

- ✓ Centro de la Cultural Plurinacional (CCP)
- ✓ Centro de la Revolución Cultural (CRC)

6.2 Ubicaciones Físicas

Las ubicaciones físicas establecidas para emprender la implementación del Plan Institucional de Seguridad de la Información de la FC-BCB, se establecen en el siguiente cuadro.

CUADRO N°2
UBICACIÓN FÍSICA DE ÁREAS ENCARGADAS DE LA IMPLEMENTACIÓN DEL P.I.S.I.

DIRECCIÓN ADMINISTRACTIVA O UNIDAD	CIUDAD	LOCALIZACIÓN
PRESIDENCIA Y CONSEJO DE ADMINISTRACIÓN	La Paz	Calle Fernando Guachalla N° 476 entre Sánchez Lima y Av. 20 de octubre
Dirección General - Unidad Nacional de Administración y Finanzas - Unidad Nacional de Asuntos Jurídicos - Unidad Nacional de Gestión Cultural - Unidad Nacional de Gestión de Infraestructura		
MUSEO NACIONAL DE ETNOGRAFÍA Y FOLKLORE	La Paz	Calle Ingavi N° 916
- Regional MUSEF – Sucre	Sucre	Calle España N° 74
MUSEO NACIONAL DE ARTE	La Paz	Calle comercio esquina socabaya
CASA NACIONAL DE LA MONEDA	Potosi	Calle Ayacucho
ARCHIVO Y BIBLIOTECA NACIONALES DE BOLIVIA	Sucre	Calle Dalence N° 4
CASA DE LA LIBERTAD	Sucre	Plaza 25 de mayo N° 11
CENTRO DE LA CULTURA PLURINACIONAL	Santa Cruz	Calle René Moreno N° 369 entre Pari y Mercado
CENTRO DE LA REVOLUCIÓN CULTURAL	La Paz	Avenida Perú - ex Estación Central

Fuente: *Elaboración Propia*

7. DIAGNÓSTICO, PRIORIZACIÓN Y GESTIÓN DE RIESGOS

Para el diagnóstico del P.I.S.I se tomó en cuenta el Plan de Implementación de Software Libre y Estándares Abiertos (PISLEA) en su Versión 1.01, para identificar activos de información y procesos críticos de la FC-BCB, Repositorios y Centro Cultural.

Se solicitó a los repositorios y centro cultural, el llenado de varios formularios que fueron enviados vía correo electrónico el 15/07/2021 según circular dirección general **FC-BCB.DG. N°007/2021**, de dicho documento se tomaron en cuenta las vulnerabilidades, amenazas que inciden en la confidencialidad, integridad y disponibilidad de la información, para llegar a una evaluación de riesgos.

Para cada uno de los procesos críticos, resultantes del análisis se identificaron actividades en las que participa para una valoración de la criticidad en función a los pilares de seguridad de

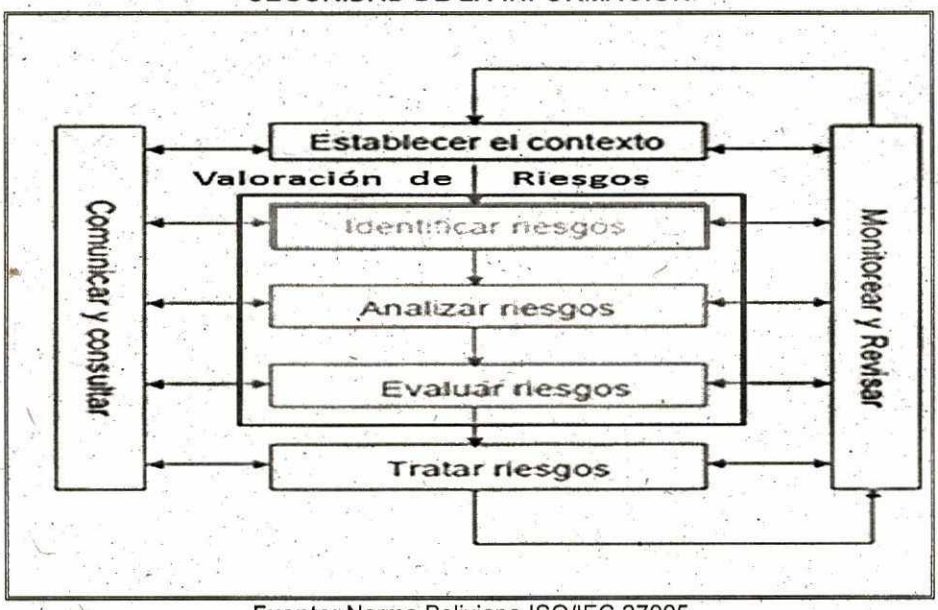
la información y se llegó a un tratamiento priorizando activos críticos y altos, para su debida revisión y elaboración de un plan de contingencia.

7.1 Gestión de Riesgos

7.1.1 Selección de Un Método de Evaluación de Riesgo

Para la evaluación del riesgo de los activos de información con los que cuenta la institución, se asumió una metodología basada en MAGERIT – Metodología de Análisis y Gestión de Riesgos de los sistemas de información Versión 3, además en el estándar de la Familia ISO 27000 de Tecnologías de la Información, Técnicas de Seguridad y Sistemas de Gestión de la seguridad de la información.

CUADRO N°3
SEGURIDAD DE LA INFORMACIÓN



Fuente: Norma Boliviana ISO/IEC 27005

7.2 Inventario de Activos de Información

De acuerdo a los lineamientos para la elaboración del P.I.S.I., la Fundación Cultural del Banco Central de Bolivia posee información crítica e importante que necesita proteger frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta vital para la institución es lo que se denomina activo de información.

Para la identificación de activos de información se utiliza la siguiente clasificación:

- ✓ **Información**
- ✓ **Claves criptográficas**
- ✓ **Servicios**
- ✓ **Software – aplicaciones informáticas**
- ✓ **Equipamiento informático (Hardware)**
- ✓ **Redes de comunicaciones**

- ✓ **Soportes de información**
- ✓ **Equipamiento auxiliar**
- ✓ **Instalaciones**
- ✓ **Personal**

En este sentido, se efectúo un inventario de activos de información tomando en cuenta al catálogo de amenazas según MAGERIT Versión 3.0, adjunto – a detalle – en el Anexo N° 1, haciendo paralelamente una clasificación de la misma, considerando los siguientes aspectos:

- Activo de información identificado
- Descripción del activo
- Clasificación del activo en base al tipo definido anteriormente
- Ubicación física del activo, es decir donde reside
- Unidad Organizacional responsable de gestionar el activo de información identificado
- Custodio, que es el encargado de tener en custodia o resguardar el activo de información
- Valoración de activos en función al nivel de afectación que tiene cada activo respecto a las dimensiones de disponibilidad, integridad y confidencialidad

El inventario efectuado, adjunto – a detalle – en el Anexo N° 2, es un resumen de los activos con los que cuenta la FC-BCB, Repositorios y Centro Cultural.

7.3 Evaluación de Riesgos

La valoración de activos de información efectuada a tiempo de la inventariación, tiene como objetivo asegurar que – producto de la actual planificación – la información reciba niveles de protección adecuados.

De forma posterior a la inventariación, se llevó a cabo el análisis y evaluación de riesgos, en el cual se determinó para cada activo de información la posibilidad de que una o varias amenazas, pueda afectar a varios procesos, ocasionando un impacto que impediría el normal funcionamiento de los procesos.

CUADRO N° 4
ESCALA DE VALORACIÓN DEL RIESGO EN LA INFORMACIÓN

Escala de Valoración	
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Fuente: *Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información*

Al respecto se han valorado las dimensiones de seguridad de información como ser: *disponibilidad, confidencialidad e integridad;* empleando los criterios de valoración que se encuentran descritos en el Anexo B punto 6.2 elaborados por la CTIC - EPB y CGII, de los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información.

Los criterios empleados, permitieron abordar los siguientes aspectos:

- ***Disponibilidad:*** *¿Qué importancia tendría que el activo no estuviera disponible?*
- ***Integridad:*** *¿Qué importancia tendría que la información asociada al activo fuera modificada sin control?*
- ***Confidencialidad:*** *¿Qué importancia tendría que la información asociada al activo fuera conocida por personas no autorizadas?*

CUADRO 5 – CRITERIO DE VALORACIÓN DISPONIBILIDAD[1]

Disponibilidad		
Valor del Activo	Clasificación	Descripción
1-MUY BAJO	Disponibilidad Muy Baja	La falla del activo de información, no inicide en la consecución de los objetivos del negocio y/o la perdida de niveles de servicio de procesos criticos.
2-BAJO	Disponibilidad Baja	La falla del activo de información, no inicide en la consecución de los objetivos del negocio y/o la perdida de niveles de servicio de procesos criticos del negocio, se considera marginal.
3-MEDIO	Disponibilidad Media	La falla del activo de información, afecta a la consecusión de los objetivos del negocio y/o incide en la perdida de niveles de servicio prestados por un proceso critico.
4-ALTO	Disponibilidad Alta	La falla del activo de información, tiene el potencial de interrumpir el negocio.
5-MUY ALTO	Disponibilidad Muy Alta	La falla del activo de información, tiene el potencial de interrumpir el negocio o afectar gravemente al niveles de servicios prestados por procesos criticos del negocio

Fuente: *Elaboración Propia con criterios Magerit versión 3.0*

CUADRO 6 CRITERIO DE VALORACIÓN INTEGRIDAD

Integridad		
Valor del Activo	Clasificación	Descripción
1-MUY BAJO	Integridad Muy Bajo	El daño o modificación no autorizada de información no es critica su impacto es insignificante.
2-BAJO	Integridad Bajo	El daño o modificación no autorizada de información no es critica para las aplicaciones del negocio y su impacto es insignificante o menor.
3-MEDIO	Integridad Media	El daño o modificación no autorizada de información es critica para las aplicaciones del negocio y su impacto en el negocio es importante.
4-ALTO	Integridad Alta	El daño o modificación no autorizada de información es critico afectando a las principales operaciones del negocio.
5-MUY ALTO	Integridad Muy Alta	El daño o modificación no autorizada de información es critico afectando a las principales operaciones del negocio, el impacto en el negocio es grave.

Fuente: *Elaboración Propia con criterios Magerit versión 3.0*

[1] Cabe hacer notar que, en los Cuadros N° 5, 6, 7 y 11 se alude a la palabra negocio, no como equivalente de empresa; sino más bien – en línea con la significancia informática – como proceso o flujo interno de trabajo de cualquier institución, el cual permite entre otros la circulación de información.

CUADRO 7 – CRITERIO DE VALORACIÓN CONFIDENCIALIDAD

Confidencialidad		
Valor del Activo	Clasificación	Descripción
1-MUY BAJO	General	Información, sistemas o instalaciones a disposición del público.
2-BAJO	Básico	Resto de contenidos
3-MEDIO	Interna	Información, sistemas o instalaciones se restringe exclusivamente para uso interno del negocio.
4-ALTO	Confidencial	Información restringida por razones de interes público
5-MUY ALTO	Clasificada	Información sensible de la organización, información clasificada.

Fuente: *Elaboración Propia con criterios Magerit versión 3.0*

Habiendo realizado la identificación de activos de la información a nivel institucional se efectuó la valoración de los mismos – adjunto en el Anexo N° 3 – identificando las vulnerabilidades, amenazas que inciden en la confidencialidad, integridad y disponibilidad de la información.

7.3.1 Criterios de evaluación del riesgo

Se evalúo las posibles consecuencias de la materialización de una amenaza producto de las vulnerabilidades presentes en los activos de información. Se estableció:

- ✓ El nivel de riesgo que cada amenaza conlleva al activo de información.
- ✓ La probabilidad de que ocurra el incidente, es decir que la amenaza explote la vulnerabilidad.
- ✓ La magnitud del impacto que el evento produce sobre el activo.

CUADRO 8
ANÁLISIS Y VALORACIÓN

ESCALAS	
PROBALIDAD	**IMPACTO**
Cierta/Inminente	Crítico
Muy Probable	Severo
Probable	Moderado
Poco Probable	Menor
Improbable	Irrelevante

Fuente: *Lineamientos para la elaboración e implementación de los PISI Anexo B 7.2*

Las amenazas y vulnerabilidades son elementos que pueden ocasionar riesgos. Las amenazas pueden ser internas o externas, usualmente las internas son de más alto riesgo, más cuando no se cuentan con medidas ni controles apropiados para mitigar el riesgo. Las vulnerabilidades son las debilidades que presenta el activo.

CUADRO 9
CATALOGO DE AMENAZAS

	ORIGEN	AMENAZA	DESCRIPCIÓN	TIPOS DE ACTIVOS AFECTADOS	DIMENSIÓN AFECTADA		
					[D] Disp	[I] Int	[C] Conf
1	Errores y fallos no intencionados	Fallas de funcionamiento de Hardware/Software por falta de mantenimiento	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	o Equipamiento informático (hardware) o Soportes de información o Equipamiento auxiliar	X		
2	Errores y fallos no intencionados	Errores del Administrador	Equivocaciones de personas con responsabilidades de instalación y operación	o Información o Claves criptográficas o Servicios o Software – aplicaciones informáticas o Equipamiento informático (hardware) o Redes de comunicaciones o Soportes de información	x	x	x
3	Errores y fallos no intencionados	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos (correo electrónico), soporte papel, etc.	o Información o Claves criptográficas o Servicios o Software – aplicaciones informáticas o Personal o Redes de comunicaciones o Soportes de información o Equipamiento auxiliar			x

				○ Instalaciones			
4	Errores y fallos no intencionados	Perdida accidental de la información digital	Ocurre porque se borró accidentalmente la información local o el equipo donde se tiene resguardada la información quedó inaccesible	○ Información ○ Claves criptográficas ○ Servicios ○ Software – aplicaciones informáticas ○ Redes de comunicaciones ○ Soportes de información ○ Instalaciones	x		
5	De origen Industrial	Sobrecargas y fluctuaciones eléctricas	Desastres debidos a la actividad humana y que afectan al suministro eléctrico	○ Equipamiento informático (hardware) ○ Soportes de información ○ Equipamiento auxiliar ○ Instalaciones	X		
6	De origen Industrial	Daños del equipamiento por acción del fuego	Posibilidad de que el fuego acabe con recursos de los sistemas	○ Equipamiento informático (hardware) ○ Soportes de información ○ Equipamiento auxiliar ○ Instalaciones	x		
7	De origen Industrial	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	○ Equipamiento informático (hardware) ○ Redes de comunicaciones	x		
8	De origen Industrial	Contaminación mecánica	Contaminación mecánica del equipamiento por	○ Equipamiento informático (hardware)	x		

			efecto del polvo, suciedad, que pueden dañar los componentes del mismo	○ Soportes de información ○ Equipamiento auxiliar			
9	De origen Industrial	Corte del suministro eléctrico	Cese de la alimentación de energía eléctrica	○ Equipamiento informático (hardware) ○ Soportes de información ○ Equipamiento auxiliar	x		
10	De origen Industrial	Degradación de los discos duros	como consecuencia de su uso y el paso del tiempo	○ Soportes de información	x		
11	De origen Industrial	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el continuo funcionamiento del sistema.	○ Software – aplicaciones informáticas ○ Equipamiento informático (hardware) ○ Soportes de información ○ Equipamiento auxiliar	x		
12	Ataques intencionados	Accesos no autorizados	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	○ Información ○ Claves criptográficas ○ Servicios ○ Software – aplicaciones informáticas ○ Equipamiento informático (hardware) ○ Redes de comunicaciones ○ Soportes de información ○ Equipamiento auxiliar ○ Instalaciones		x	x
13	Desastres Naturales	Desastres Naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto,	○ Equipamiento informático (hardware) ○ Soportes de información	x		

			ciclones, avalancha, corrimiento de tierras, etc.	○ Equipamiento auxiliar ○ Instalaciones			
14	Ataques intencionados	Denegación de Servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	○ Servicios ○ Equipamiento informático (hardware) ○ Redes de comunicaciones	x		
15	Errores y fallos no intencionados	Agotamiento de recursos	La carencia de recursos suficientes provoca la caída o malfuncionamiento del sistema cuando la carga de trabajo es desmesurada.	○ Servicios ○ Equipamiento informático (hardware) ○ Redes de comunicaciones	x		
16	Errores y fallos no intencionados	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. Falta de implementación de técnicas de desarrollo seguro. Falta de actualizaciones de los sistemas operativos	○ Software – aplicaciones informáticas	x	x	x
17	Errores y fallos no intencionados	Errores de mantenimiento de las aplicaciones y programas	Falta de mecanismos y procedimientos de actualización y aplicación de parches de seguridad a las plataformas y librerías utilizadas	○ Software – aplicaciones informáticas	x	x	x

18	Errores y fallos no intencionados	Errores de monitorización	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	○ Registros de actividad		x	
19	Errores y fallos no intencionados	Uso de contraseñas débiles	Falta de mecanismos de seguridad en la definición de las contraseñas de los sistemas aplicativos (mínimo 6 caracteres, caracteres alfa numéricos, tiempo de validez de la contraseña, intentos fallidos, etc.)	○ Software – aplicaciones informáticas ○ Equipamiento informático (hardware) ○ Redes de comunicaciones			x

Fuente: *Elaboración Propia*

En base al nivel de cada riesgo identificado, el Cuadro N°10 muestra los respectivos mapas de riesgos.

CUADRO 10
MODELO DE MATRIZ DE VALORACIÓN DE RIESGOS

PROBABILIDAD						
	CIERTA/INMINENTE	BAJO	MEDIO	ALTO	CRÍTICO	CRÍTICO
	MUY PROBABLE	BAJO	MEDIO	ALTO	ALTO	CRÍTICO
	PROBABLE	IRRELEVANTE	BAJO	MEDIO	ALTO	ALTO
	POCO PROBABLE	IRRELEVANTE	BAJO	BAJO	MEDIO	MEDIO
	IMPROBABLE	IRRELEVANTE	IRRELEVANTE	IRRELEVANTE	BAJO	BAJO
		IRRELEVANTE	MENOR	MODERADO	SEVERO	CRÍTICO
		IMPACTO				

Fuente: *Elaboración Propia con criterios Magerit versión 3.0 inciso 2.1. Análisis mediante tablas*

Del cuadro referido, se puede apreciar cinco (5) niveles de riesgo: Irrelevante, bajo, medio, alto y crítico. Las amenazas, riesgos y vulnerabilidades que se encuentran en los riesgos alto y crítico deben ser tratados para minimizar su impacto, los riesgos que se encuentran en un nivel de riesgo medio, bajo e irrelevante no serán tratados, salvo que por decisión del Comité de Seguridad de la Información sea conveniente su trato.

Habiendo realizado la identificación de riesgos de la FCBCB en los activos de información identificados producto de la inventariación, se efectuó la valoración de riesgos – adjunta en el Anexo N° 5 – de la cual resalta el hecho de los sistemas críticos y altos en nivel de riesgo que pueden llegar a impedir la continuidad de los servicios que esta proporciona a la institución.
Se muestran 13 activos, resultado del análisis del anexo II y tomando en cuenta la valoración final y comparando los datos con la escala de valoración del riesgo en la información (Cuadro 4).
Posteriormente de la información recolectada de todas las Áreas Organizacionales que integran la FC-BCB se efectuó la priorización de 7 activos de información, tomando en cuenta los datos del nivel de riesgo y comparándolos con el modelo de matriz de valoración de riesgos (Cuadro 9).

7.4 Tratamiento del Riesgo

Una vez identificados y evaluados los riesgos, se delinean las propuestas de tratamiento respectivo, en ese contexto se cita las siguientes categorías de acción:

- **Aceptar el riesgo:** Se asume el riesgo debido a que la misma está por debajo del valor de riesgo aceptable, simplemente requiere que quede documentado. Los riesgos que se han asumido deben ser controlados y revisados periódicamente, de cara a evitar que evolucionen y se conviertan en riesgos mayores.
- **Reducir el riesgo:** Reducir el riesgo a un nivel aceptable mediante la implantación de controles establecidos en los Lineamientos para la Elaboración e Implementación del P.I.S.I, el cual implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.
- **Retener el riesgo:** Implica establecer criterios para su aceptación, no es necesario implementar o seleccionar controles adicionales si el riesgo puede ser retenido.
- **Evitar:** El riesgo puede evitarse cuando este se considera muy alto, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios. Se puede tomar una decisión que logre evitar por completo el riesgo, mediante el retiro de una actividad, condiciones o conjunto de actividades ya sean planificadas o existentes. Esto deberá estar debidamente justificado y documentado.
- **Transferir el riesgo:** Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

Para el caso de activos de información se asume el riesgo, los riesgos identificados son (7) priorizados y de acuerdo a su criticidad se realizó a identificar el tipo de tratamiento en función a los controles establecidos por la CTIC - EPB y CGII, Cuadro 11.

CUADRO 11
VALORACIÓN DE RIESGOS

Valor del Activo	CRITICIDAD	Descripción
[1-3]	IRRELEVANTE	Activo de información irrelevante para el proceso o negocio.
[4-6]	BAJO	Activo de información que no es prioritario para el proceso o el negocio (consecución de objetivos).
[8-10]	MEDIO	Activo de información que se considera de valoración media para el proceso o el negocio (consecución de objetivos)
[12-16]	ALTO	Activo de información que se considera importante para el proceso o el negocio (consecución de objetivos)
[20-25]	CRÍTICO	Activo de información que se considera imprescindible para el proceso o el negocio (consecución de objetivos)

Fuente: *Elaboración Propia con criterios Magerit versión 3.0*
Negocio=Referente al flujo de trabajo de la entidad FCBCB

En función a estas amenazas, se evaluó el impacto en el activo tecnológico, para la amenaza identificada se determinó tipos de controles y acciones para mitigar el riesgo de los siete (7) activos, aquellos que, de acuerdo a Lineamientos presentaron riesgos altos (color naranja) y críticos (color rojo), mismos que deberán ser tratados de acuerdo al cronograma de implementación. Del Anexo N° 5 – adjunto al presente documento – resalta el hecho de la mitigación de los activos críticos y altos, llegando a un tratamiento, para la disminución del riesgo, implementando controles, revisiones y planes de contingencia. Se calculó el nivel de riesgo inherente en base a la siguiente formula:

Riesgo = Probabilidad x Impacto

Se realizó la valoración de la métrica eficiencia y efectividad de los controles existentes, validando si el control aplicado permite disminuir el impacto.

7.5 Controles Implementados y por Implementar

Los controles implementados y por implementar producto del P.I.S.I. representa la base para la aplicación de las directrices y actividades de los lineamientos normativos que se aplican a los límites y alcance establecido, asimismo permite justificar aquellos controles que no van a ser implementados. Con el objeto de lograr este objetivo, se realizó el análisis y desarrollo

mediante el uso del formulario de matriz de controles implementados y por implementar, tomando como referencia base los riesgos identificados, las normativas regulatorias internas o externas y las necesidades del proceso en el alcance del plan, mismos que figuran en el Anexo N°5 Identificación, Análisis y Valoración de Riesgos, donde:

***D**=Disponibilidad, **I**=Integridad, **C**=Confidencialidad*

La valoración final se obtiene en base a la siguiente ecuación:

Valoración de riesgo= (D+I+C) /3

Valoración Final=(D+I+C)

La valoración de la probabilidad y el impacto vienen dadas por la siguiente tabla:

PROBALIDAD	IMPACTO	VALOR
Cierta/Inminente	Crítico	5
Muy Probable	Severo	4
Probable	Moderado	3
Poco Probable	Menor	2
Improbable	Irrelevante	1

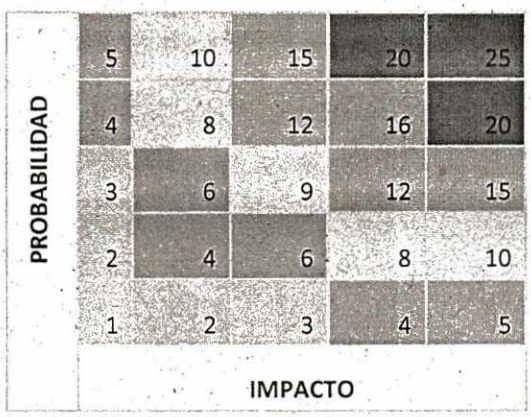
Donde:

Probabilidad= P, **Impacto**=IM

Una vez identificados los valores de la probabilidad e impacto para el cálculo del riesgo se hace uso de la siguiente formula:

Riesgo=P*IM

Cuyo valor es identificado en la siguiente matriz de valoración de riesgos:



Este valor numérico se traduce en la valoración de criticidad establecida en el Cuadro N° 11 del presente documento.

8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

8.1 Objetivo General

La Política de Seguridad de Información de la FC-BCB, tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información generada en los procesos internos y externos de la FC-BCB, a través de la protección de los activos, operaciones y procesos vinculados con el flujo de información.

8.2 Objetivos Específicos

La Política de Seguridad de Información de la FC-BCB, persigue internamente y de manera específica los siguientes objetivos:

a) Integrar y preservar la información institucional, a partir de la gestión de activos de la información, gestión de riesgos y/o incidentes, orientadas a controlar y preservar los datos de valía institucional que contribuyen a los procesos y/o servicios internos y externos.
b) Garantizar el flujo seguro de información institucional que permita el óptimo desarrollo de la vocación institucional y contribuya – desde los procesos internos – a poner en valor, preservar, conservar y promocionar el patrimonio cultural y expresiones artísticas a nivel local, nacional e internacional.
c) Garantizar la disponibilidad e integridad de la información, que facilite y posibilite el eficiente cumplimiento de la gestión técnica, humana y administrativa y financiera transparente y eficiente de la institución.
d) Aplicar de manera efectiva los paradigmas de buenas prácticas de seguridad en el desarrollo de sistemas para la generación de políticas necesarias en la Fundación Cultural del Banco Central de Bolivia, para mitigar los riesgos de información identificados.
e) Mantener la confidencialidad de la información en los sistemas desarrollados internamente y/o por terceros, para evitar riesgos que sean ocasionados por partes externas.

8.3 Roles y Responsabilidad

- **[RSI],** El Responsable de Seguridad de la Información, con perfil y experiencia en gestión de seguridad de la información, es designado por la MAE, y tiene como función principal la elaboración e implementación del PISI, y como funciones específicas, las siguientes:

  a) Gestionar, elaborar e implementar el Plan Institucional de Seguridad de la Información (PISI).
  b) Realizar la evaluación de riesgos de seguridad de la información en coordinación con los responsables de activos de información.
  c) Proponer la Política de Seguridad de la Información (PSI), que estará incorporada dentro del PISI.

d) Gestionar el cumplimiento del PISI.
e) Elaborar manuales de procesos y/o procedimientos de seguridad específicos que se desprendan de los lineamientos del Plan Institucional de Seguridad de la Información y promover su difusión en la entidad o institución pública.
f) Sugerir prácticas de desarrollo de software seguro para generar procesos formales que tengan presentes los controles de seguridad necesarios para la entidad o institución.
g) Coordinar la inducción, capacitación y comunicación del personal, en el marco del PISI.
h) Gestionar y coordinar la atención y respuesta a incidentes de seguridad de la información en su entidad o institución.
i) Coadyuvar en la gestión de contingencias tecnológicas.
j) Proponer estrategias y acciones en mejora de la seguridad de la información.
k) Promover la realización de auditorías al Plan Institucional de Seguridad de la Información.
l) Gestionar la mejora continua de la seguridad de la información.
m) Sugerir medidas de protección ante posibles ataques informáticos que puedan poner en riesgo las operaciones normales de la Institución.
n) Realizar acciones de informática forense, en caso de ser necesario, para identificar, preservar, analizar y validar datos que puedan ser relevantes.
o) Monitorear la implementación y uso de mecanismos de seguridad, que coadyuven a la reducción de los riesgos identificados.
p) Otras funciones que resulten necesarias para preservar la seguridad de la información.

- **[CSI],** El Comité de Seguridad de la Información, es un equipo de trabajo conformado para gestionar, promover e impulsar iniciativas en seguridad de la información. Sus integrantes son designados mediante Resolución Administrativa, de acuerdo al tamaño de la estructura organizativa de su entidad, volumen y complejidad de sus operaciones. El CSI estará conformado por:
  - La Máxima Autoridad Ejecutiva en calidad de presidente del CSI, con la posibilidad de delegar sus funciones.
  - Personal de nivel jerárquico, de acuerdo a la estructura organizativa de la entidad o institución pública.
  - El Responsable de Seguridad de la Información (RSI).

En caso de la existencia de Comités similares, se considerará la posibilidad de que estos asuman las funciones del CSI.
El CSI debe desarrollar las siguientes funciones:

a) Revisar el Plan Institucional de Seguridad de la Información (PISI).
b) Promover la aprobación del PISI a través de la MAE.

c) 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.
d) Proponer estrategias necesarias para la implementación y/o fortalecimiento de controles de seguridad en el marco de la mejora continua.
e) Realizar el seguimiento y control de los indicadores y métricas establecidos y definir las acciones que correspondan al respecto.
f) Promover la concientización y capacitación en seguridad de la información al interior de la entidad o institución pública.
g) 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.
h) Otras funciones que resulten necesarias para la seguridad de la información.

- **[MAE],** tiene la responsabilidad de aprobar y revisar a intervalos regulares la Política Institucional y Procedimientos de Seguridad de Información.
- **[Direcciones de Área y Direcciones Administrativas],** tienen la obligación de promover el cumplimiento de las Política Institucional y Procedimientos de Seguridad de Información.
- **[Servidoras y Servidores Públicos]**, son responsables de dar cumplimiento estricto a la Política y Procedimientos de Seguridad de Información; también se establece la responsabilidad para coadyuvar de manera efectiva a la implementación del Plan Institucional de Seguridad de Información (PISI).
- **[Auditoría Interna]**, debe practicar auditorías periódicas respecto el cumplimiento normativo en relación a la adopción e implementación del Plan Institucional de Seguridad de Información en la institución.

8.4 Ámbito de Aplicación

En este documento se formulan los lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información y las directrices técnicas para la aplicación de controles de seguridad de la información.

Las determinaciones adoptadas en la presente Política, son de aplicación obligatoria por parte de todas las Áreas Organizacionales dependientes de la Fundación Cultural del Banco Central de Bolivia (FC-BCB), de acuerdo a normativa vigente.

8.5 Marco Regulatorio

La Fundación Cultural del Banco Central de Bolivia se encuentra sujeta al cumplimiento normativo nacional en materia de seguridad de la información, el cual – en conjunto – establece lineamientos relacionados al adecuado resguardo y confidencialidad de la información y al uso eficiente de los activos tecnológicos con los que cuenta.

A continuación, se exponen, las directrices normativas principales:

- Política de la seguridad de la información
- Reglamento Interno del Personal

- Constitución Política del Estado
- Ley N° 1670 del BCB
- Estatuto de la FC-BCB
- Decreto Supremo N°2514
- Resolución Administrativa N° 051/2017

La Constitución Política del Estado, en su artículo 103, parágrafo 2, establece que "El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación". Asimismo, con la Ley General de Telecomunicaciones, N° 164, en su Parágrafo I del Artículo 72, se define 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 de 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".

El Decreto Supremo N° 2514 de 9 de septiembre de 2015, en su parágrafo III del Artículo 17, establece que "Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII".

El Estatuto de creación de la FC-BCB en su Artículo 3, I) establece: "La FC-BCB tiene la tuición y administración de la Casa Nacional de la Moneda (Potosí), El Archivo y Biblioteca Nacionales de Bolivia (Sucre), el Museo Nacional de Etnografía y Folklore (La Paz), el Museo Nacional de Arte (La Paz) y el Centro de la Revolución Cultural (Santa Cruz), sin que estos Repositorios Nacionales pierdan su condición de patrimonio cultural e histórico del Estado Plurinacional de Bolivia; y II) Los Repositorios Nacionales y Centros Culturales, en su funcionamiento dependen de la FC-BCB y de sus Órganos de Dirección y cumplen las funciones y servicios que les asignan las normas legales en vigencia.

La normativa interna de la FC-BCB refiere que la misma ejerce tuición sobre los Repositorios Nacionales y Centros Culturales, entendidos estos como Direcciones Administrativas; y que por lo tanto su planificación y funcionamiento comparten una sola lógica, por lo que se delinea un Plan Institucional de Seguridad de la Información (PISI) para la FC-BCB y sus dependencias, con connotaciones particulares de acuerdo a las características físicas de cada Dirección Administrativa.

8.6 Clasificación de la Información

La FC-BCB clasificará su información en función de los siguientes parámetros:

a) **Información confidencial:**
Esta información es de nivel crítico, aspecto que determina que su acceso sea de conocimiento de la MAE, Direcciones de Área y Direcciones Administrativas por ello debe ser manejada y protegida con mayor atención.

b) **Información privada:**
Esta información solo puede ser de conocimiento de los funcionarios públicos para el desempeño de sus funciones, el envío de dicha información a terceros debe ser autorizado por las instancias que correspondan.

c) **Información pública:**
Esta información es de conocimiento público y su divulgación al interior o al exterior de las diferentes Áreas Organizacionales de la FC-BCB, no representa un impacto negativo de orden competitivo, reputación o sancionable.

8.7 Seguridad en Recursos Humanos

La FC-BCB en el marco de la Gestión de Seguridad de Información y de los recursos humanos, dispone:

a) **Responsabilidades,** las responsabilidades en el marco de seguridad de la información deben ser conocidas y aceptadas formalmente, por los servidores públicos.

b) **Formación y capacitación,** la instancia Responsable de Seguridad de Información (RSI), establecerá un programa permanente para la formación y capacitación en materia de seguridad, para todos los servidores públicos, personal eventual, consultores o cualquiera que tenga un vínculo laboral con la FCBCB a objeto de generar una cultura de seguridad de información en la entidad.

c) **Acuerdos de Confidencialidad,** todos los servidores públicos, personal eventual, consultores o cualquiera que tenga un vínculo laboral con la FCBCB, deben firmar un compromiso para la protección, buen uso y preservación de la información más sensible de la institución. Se sancionará el uso negligente de la información.

d) **Remoción de los derechos de acceso,** toda vez que se produzca la desvinculación de un servidor público, personal eventual, consultores o cualquiera que tenga un vínculo laboral con la FC-BCB, se deben cancelar inmediatamente los derechos de acceso a los sistemas de información y servicios tecnológicos.

e) **Sanciones por el incumplimiento de la Política de Seguridad de Información,** se debe establecer formalmente las sanciones, por el incumplimiento de la presente política de seguridad de información.

f) **Circuitos de control de acceso y vigilancia sobre el acceso a internet**, se debe efectuar un monitoreo constante de la red local y externa sobre los accesos en intentos de acceso a información confidencial.

8.8 Gestión de activos de información

Para mantener una apropiada protección de los activos y garantizar que los mismos reciban un nivel apropiado de seguridad, las Áreas Organizacionales de la FC-BCB contaran con:

a) Un inventario todos los activos de información dentro de los alcances del PISI.

b) Será asignado para cada activo de información un responsable y/o custodio de acuerdo a sus funciones y competencias.
c) Se establecerá las restricciones y condiciones de uso adecuado de activos de información.
d) Se precautelará la disponibilidad, integridad y confidencialidad de los activos de información al momento de la desvinculación o cambio de cargo previa documentación
e) En caso de desvinculación, la devolución del activo de la información se hará previa revisión del estado de la información con documentación previa
f) Protección de la documentación será bajo responsabilidad del funcionario mientras este en ejercicio del cargo.
g) En la gestión de medios removibles, USB, discos externos, dispositivos móviles y otros estos estarán sujetos a autorizaciones de los encargados de resguardar la información

Se elaborará e implementará un reglamento para el manejo de información, de acuerdo con el esquema de gestión de activos de la información.

8.9 Control de accesos

Se elaborará e implementará un procedimiento de registro formal para el alta, baja de usuarios que garantice la asignación y la revocación de accesos a todos los sistemas y servicios, además de revisiones periódicas al respecto se implementarán los siguientes controles:

a) **Registro de usuarios,** se debe contar con registros de la Alta, Baja y/o Modificación de los derechos de acceso a servicios, sistemas y aplicaciones.
b) **Usuarios Externos,** las cuentas de usuarios externos para el acceso a los sistemas de la información deben tener caducidad no superior a seis (6) meses renovables de acuerdo a la naturaleza del usuario.
c) **Gestión de contraseñas**, las claves serán, alfanuméricas, estableciendo un mínimo de caracteres y caducidad, se modificará periódicamente facilitando su seguridad.
d) **Acceso Remoto,** se deben utilizar métodos de autenticación seguros para controlar el acceso de usuarios remotos.
e) **Gestión de privilegios,** deben restringirse y controlarse la asignación y el uso de privilegios en los sistemas y redes.
f) **Revisión de derechos de acceso y privilegios,** deben revisarse periódicamente los privilegios y derechos de acceso de los sistemas de información y servicios de tecnología, para limitar accesos no autorizados. Esta revisión será efectuada en función de las desvinculaciones efectuadas de los servidores públicos y/o cambios en los niveles o cargos al interior de la institución.
g) **Control de acceso a la red,** deben definirse controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.
h) **Identificación de equipos de red,** deben identificarse ubicaciones específicas y conexiones de equipos.
i) **Acceso a Internet,** el acceso al internet deberá ser controlado y su acceso deberá corresponder con la naturaleza de la función desempeñada por los servidores públicos.

j) **Acceso a redes inalámbricas,** se controlará el acceso a redes wifi mediante protocolos de autenticación robustos y segregación de redes según en función a las necesidades.

k) **Acceso de dispositivos móviles,** se entregará a los usuarios un detalle escrito de sus derechos de accesos a la información a través de teléfonos móviles.

8.10 Criptografía

Se elaborará e implementará un reglamento para asignar y administrar la información criptográfica, incluye toda la información almacenada en dispositivos y hardware, así como la información custodiada en espacios de archivo o copia de seguridad, deberán contar con cifrado AES o RSA, debiendo tener en cuenta la siguiente consideración:

a) Toda información de carácter confidencial y o restringida, debe ser almacenada y/o transmitida con mecanismos de encriptación de datos para prevenir la perdida de confidencialidad.

8.11 Seguridad física y ambiental

Se elaborará un reglamento para verificar que la seguridad física y ambiental se encuentran en óptimas condiciones de operación. A fin de preservar la seguridad física de las instalaciones, se tomarán en cuenta las siguientes consideraciones:

a) Zonas de Exclusión, es decir zonas de acceso restringido, se implementará controles de seguridad, para prevenir accesos no autorizados. Según sea necesario, se implementará los siguientes controles:

- Control de acceso biométrico
- Sistemas de monitoreo y vigilancia
- Detector de humo
- Extintor de fuego
- Sistema de Alarma

b) Centro de procesamiento de datos, el cual deberá tener las siguientes características:

- Espacio acorde y suficiente.
- Energía regulada.
- El cableado deberá cumplir con los estándares de cableado estructurado.
- No almacenar papel u otros suministros inflamables y/o equipos en desuso.
- Instalación de los servidores y los equipos de comunicación de forma independiente, debidamente asegurados, según corresponda.
- Sistema de Climatización
- Detector de Humedad
- Los ingresos y salidas de visitas deberán ser registradas, autorizadas y controladas.

c) Seguridad del equipamiento informático y el software, no se deberán retirar de las instalaciones sin previa autorización, para ello se debe establecer responsables y responsabilidades.

La información almacenada en los equipos asignados para el uso de los funcionarios debe ser respaldada con copias de seguridad periódicamente, en lo posible se debe implementar

controles de seguridad periódicos de equipos asignados al personal para casos de extravío o hurto.

d) Escritorios y pantallas limpias, en instalaciones de atención al público se deberá mantener el escritorio despejado así mismo se debe bloquear la pantalla cuando se encuentre sin supervisión, finalizar sesiones activas en aplicaciones o servicios de redes cuando no sean utilizadas a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

8.12 Seguridad de las operaciones

Las operaciones y la gestión de tecnologías de información deben ser formalmente establecidas y controladas, al respecto se deben implementar los siguientes procedimientos:

a) Responsabilidad de las operaciones, se deberá identificar los procesos operacionales relacionados a la seguridad de la información, para documentar la instalación, configuración, recuperación, reinicio y mantenimiento de Infraestructura Tecnológica.

b) Gestión de Cambios, el RSI será el responsable para la aprobación de cambios.

c) Gestión de capacidad, al menos una vez al año se deberá evaluar, revisar y eliminar los datos obsoletos almacenados, así como dar de baja a las aplicaciones, sistemas, bases de datos o entornos en desuso y/o obsoletos.

d) Respaldos, la información en base a su nivel de criticidad, disponibilidad y confidencialidad, requiere ser protegida mediante la obtención de copias de respaldo.

e) Toda la información respaldada debe poseer un nivel adecuado de protección lógica, física, en un ambiente físico destinado al resguardo, que garantice mínimamente la protección contra daño, deterioros y hurto. Todos los programas, paquetes de software deben estar acompañados de sus manuales y ser almacenados en un ambiente de resguardo seguro y controlado.

8.13 Seguridad de las comunicaciones

La gestión de comunicaciones, está orientada a prevenir, diagnosticar y resolver problemas de la red, asimismo brindar a los usuarios una red como entorno fiable, seguro, rápido y operacional.

Con tal propósito la gestión de redes y comunicaciones pretende optimizar:

a) Gestión de la red
b) Seguridad en servicios de red
c) Seguridad en la red perimetral, el hardware perimetral debe contar con un cifrado estándar, aspecto que garantizará la integridad de la información en la red interna, la transferencia de información debe estar encriptada a nivel de protocolo. Se debe realizar un monitoreo constante de la red interna y externa tanto de datos y de voz, verificando la disponibilidad de los servicios y de los recursos tecnológicos. Se debe

medir periódicamente ruido en la carga de paquetes, con escaneos de la red, paquetes perdidos e informes de errores o fallos.

d) Segmentación de la red, se debe segmentar el dominio institucional interno (DNS interno) del dominio institucional externo (DNS externo).
e) Seguridad en redes WiFi
f) Transferencia de información, generando procesos de aseguramiento que contemplen acuerdos de confidencialidad, protocolos de seguridad, entre otros, SSL (Secure Sockets Layer) que permite dar y recibir claves de cifrado.
   Los criterios de seguridad para la transferencia de datos deben ser actualizados de manera permanente.

Se elaborará un reglamento para la seguridad de las comunicaciones, que contendrá documentación técnica actualizada de cada infraestructura de red y su seguridad. Además, que contemple mínimamente la verificación positiva de direcciones de origen y destino, y adicionalmente diversos métodos incluyendo entre otra autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

8.14 Desarrollo, mantenimiento y adquisición de sistemas

Los sistemas de información deben contar con controles que garanticen el funcionamiento de los sistemas informáticos, en todas las etapas de desarrollo, pruebas e implementación o puesta en marcha.

Se elaborará un reglamento para la construcción de nuevos sistemas de información o mejoras a los existentes, que comprenda la etapa de diseño, las pruebas de sistemas, validación de datos, control de cambios para los sistemas de información en producción controlando la integridad de los mismos, para este propósito se debe tener en cuenta los siguientes controles:

a) **Documentación de Sistemas de Información**, la documentación de sistemas es el conjunto de información que nos dice qué hacen los sistemas, cómo lo hacen y para quién lo hacen. La documentación consiste en material que explica las características técnicas, procedimientos técnicos y la operación de un sistema. Todo desarrollo de programa debe contar con documentación técnica del programa informático, bibliotecas, diccionarios del código fuente y programas ejecutables.
   Todo desarrollo de programas informáticos o sistemas informáticos adquiridos de terceros por las Áreas Organizacionales de la FC-BCB, debe contar con la documentación técnica o soporte técnico que permita brindar la continuidad del programa o sistemas en caso de interrupciones o contingencias presentadas por diferentes situaciones.
   La información de los códigos fuente y programas debe contar con la adecuada protección y se deberá establecer un procedimiento para su custodia segura.
b) **Versionamiento de software,** todo desarrollo de programa debe contar con un registro de la versión y cada vez que se realice alguna modificación, debe ser actualizado el número de versión. Los desarrollos realizados por terceros deben adecuarse al

lineamiento establecido por la Fundación Cultural del Banco Central de Bolivia FC-BCB y de todos sus Repositorios Nacionales y Centros Culturales.

c) **Controles de acceso a la base de datos,** se debe contar con controles de acceso a las bases de datos, el mismo debe establecer criterios de autenticación y autorización, evitando modificaciones no controladas.
d) **Pruebas en ambientes diseñados para pruebas,** el ambiente de pruebas debe contar con una base de datos de pruebas, a efectos de evitar distorsiones en la información que se encuentra en producción. Se debe establecer un control de calidad del programa informático desarrollado antes de su puesta en producción.
e) **Puesta en producción e implementación,** el software desarrollado puesta en funcionamiento para la mejora de la implementación tecnológica en función de las diferentes áreas comprometidas para con los sistemas tecnológicos.

8.15 Gestión de incidentes de seguridad de la información

En caso de que se produzca incidentes de seguridad en las dependencias de la Fundación Cultural del Banco Central de Bolivia (FC-BCB). En aplicación del Decreto Supremo N° 2514 Artículo 8 se debe seguir los siguientes pasos:

a) **Designación de responsable. -** La Fundación Cultural del Banco Central de Bolivia debe designar un Responsable de Seguridad de la Información (RSI).
b) **Identificación. -** El RSI debe solicitar a todas las áreas de la FCBCB una identificación y reporte en un periodo previamente coordinado, de los incidentes informáticos sucedidos.
c) **Reporte. -** El RSI debe reportar oportunamente los incidentes de seguridad de información sucedidos al *Centro de Gestión de incidentes informáticos* de la AGETIC.
d) **Clasificación y registro. -** el RSI debe clasificar y mantener un registro de incidentes de seguridad de información.
e) **Contención y Respuesta. -** todo incidente de seguridad de información debe ser valorado, siendo competencia del RSI en la contención y respuesta en los activos de la información, así también si corresponde se debe solicitar el Soporte técnico por parte del CGII.

8.16 Plan de contingencias tecnológicas

Las Direcciones de Área y Direcciones Administrativas deben delegar un responsable para que coordine las otras áreas de la Fundación Cultural del Banco Central de Bolivia (FC-BCB), y a su vez identifique los activos críticos, la valoración del riesgo, el tratamiento del riesgo y la aceptación de ciertos niveles de riesgo, así como proponer planes de contingencia tecnológicos de acuerdo con los siguientes criterios:

- El análisis y evaluación de riesgos en seguridad de la información.
- La Gestión de Incidentes de Seguridad de la Información.
- La identificación de los escenarios de riesgo que afecten la infraestructura tecnología y operación de los servicios tecnológicos.

- Cada Plan de Contingencias Tecnológicas deberá describir el enfoque para la continuidad, así como las condiciones necesarias para activar un plan de escalamiento si fuese necesario.
- Implementar procedimientos de recuperación y restauración de operaciones críticas para cada escenario de riesgo identificado.

8.17 Indicadores y métricas

Los indicadores y métricas empleados al momento de identificar criticidades, así como elaborar y desarrollar el control de seguridad de nuestro Plan de Seguridad de la Información, serán aplicadas también a tiempo de evaluar la eficacia de los controles implementados en los activos priorizados.

Cada Repositorio Nacional y Centro Cultural de la FC-BCB, tiene sus riesgos, por tanto, se necesita métricas vinculadas a los objetivos de seguridad y los procesos necesarios específicos. Los indicadores aplicados a la valoración inicial, que serán aplicados – a su vez – para medir la reducción de la criticidad en los activos priorizados, se encuentran inmersos en:

- Identificar los Activos de información. (Ver ANEXO II)
- Realizar un análisis de riesgos bajo una metodología de riesgos identificando los riesgos y amenazas en cada uno de los activos de información. (Ver ANEXO III y IV)
- Identificar el nivel de seguridad existente en los sistemas, servicios, aplicaciones e infraestructura (incidentes, actualizaciones) (Ver ANEXO V)
- Definir y planificar los planes de acción a realizar (a corto, mediano y largo plazo). (Ver Cronograma de implementación)
- Implementar mecanismos de seguridad, con los siguientes controles:
    1. Seguridad en recursos Humanos
    2. Gestión de activos de la información
    3. Control de accesos
    4. Criptográfica
    5. Seguridad física y ambiental
    6. Seguridad de las operaciones
    7. Seguridad de las comunicaciones
    8. Desarrollo, mantenimiento y adquisición de sistemas
    9. Gestión de incidentes.

Las métricas utilizadas consistirán en medidas definidas y adaptadas, tanto a nivel estratégico (progreso del cronograma) como táctico y operativo (procesos y controles de la Política de seguridad de la información). En cada nivel las métricas deben tener las propiedades de ser:

a) Específico
b) Medible cualitativa o cuantitativamente y/o con indicadores y atributos.
c) Alcanzable.

d) Relevante.
e) Repetible en periodos de tiempo.

La métrica va a indicar el grado en el que se cumplen nuestros objetivos de seguridad, por ello utilizamos la métrica Eficacia o efectividad.

- **Eficacia o efectividad:** Porcentaje de disminución de los riesgos.

8.18 Cumplimiento

La presente Política de Seguridad de Información es de cumplimiento obligatorio para todo servidor público dependiente de la Fundación Cultural del Banco Central de Bolivia FC-BCB y de todas sus Áreas organizacionales.

9. DIFUSIÓN

La presente Política de Seguridad de Información, se difundirá de manera específica a cada Área Organizacional y a los servidores específicos encargados de su implementación, y estará disponible a través de la página web institucional para todos los servidores públicos de la FCBCB, debe contener y describir la posición institucional en cuanto a la difusión de toda la documentación generada a partir de ella, así como los medios y mecanismos de su difusión.

10. SANCIONES

El incumplimiento o la violación de las disposiciones de la presente Política de Seguridad de Información y los potenciales efectos adversos para la organización serán valorados en aplicación del Reglamento Interno de Personal (RIP) de la Fundación Cultural del BCB, específicamente en cuanto a:

- **Artículo 11 DEBERES CON LA ENTIDAD**, que en el inciso d) señala que es *"Desarrollar sus labores o tareas y manejar documentación e información a su cargo con responsabilidad y diligencia"*
- **Articulo 41 FALTAS Y SANCIONES** que indica:

  "i. Las faltas cometidas por el personal de la entidad en contra de lo establecido por el presente Reglamento interno, así como a la normativa jurídica y administrativa para el sector público, se clasifican en función al grado de afectación que estas tengan sobre la gestión pública de la entidad, así como por su recurrencia.

  Las faltas de clasifican en: Leves, Graves y Gravísimas

  ii. Las sanciones a las faltas cometidas por el personal de la entidad, estarán establecidas en normativa o serán determinadas como consecuencia de Proceso Sumario Administrativo. Las sanciones podrán ser administrativas y/o económicas."

11. HISTÓRICO DE CAMBIOS

Se recomienda que la documentación generada a partir de la PSI cuente con el respectivo control de cambios, el cual consigne información referente a:

- Versión del documento.
- Modificación del documento.
- Servidor (es) Público (s) encargados de la modificación.
- Elaboración de una nueva versión de la política de la información.
- Documentar el control de cambios de acuerdo a las versiones de la planificación.

12. CRONOGRAMA DE IMPLEMENTACIÓN

N°	ACTIVO DE INFORMACIÓN PRIORIZADO	CONTROLES A IMPLEMENTARSE	ACCIONES A DESARROLLAR	FECHA DE INICIO	FECHA DE CONCLUSIÓN	RESPONSABLES	REQUERIMIENTO PARA LA IMPLEMENTACIÓN DE LA ACCIÓN
1	*Sistemas de Correspondencia*	1. PISI 8.14 2. PISI 8.16	1. Implementar una política y un procedimiento para contingencias tecnológicas.	01/09/2021	01/09/2022	- Personal de Sistemas de planta y/o consultores. - RSI	Aplicación de control de correspondencia
2	*Sistema Contabilidad Visual*	1. PISI 8.14 2. PISI 8.16 3. PISI 8.15	1. Implementar políticas y procedimientos para contingencias tecnológicas.	01/09/2021	01/09/2022	- Personal de Sistemas de planta y/o consultores. - RSI, Jefes Administrativos Financieros	Adquisición de equipos para el Sistema Contabilidad visual (Servidores) en cada Área Organizacional
3	*Mantenimiento de Sistemas de Información*	1. PISI 8.14	1. Implementar políticas y procedimientos de clasificación de información.	01/09/2021	01/09/2022	- Personal de Sistemas de planta o consultores. - RSI, Jefes de Unidad	Capacitación al personal de la enidad respecto a

N°	ACTIVO DE INFORMACIÓN PRIORIZADO	CONTROLES A IMPLEMENTARSE	ACCIONES A DESARROLLAR	FECHA DE INICIO	FECHA DE CONCLUSIÓN	RESPONSABLES	REQUERIMIENTO PARA LA IMPLEMENTACIÓN DE LA ACCIÓN
			2. Mantenimiento en los sistemas de información: Hardware, Software y documentación				seguridad de información.
4	*Servidores*	1. PISI 8.11 Inciso b) 2. PISI 8.11 Inciso b) 3. PISI 8.13 Inciso a), b) y d) 4. PISI 8.11Inciso b), c) 5. PISI 8.9 Inciso b) 6. PISI 8.12 7. PISI 8.11 Inciso a)	1. Implementar sistema de Climatización 2. Implementar UPS control de picos 3. Implementar segmentación de redes & VLAN 4. Implementar sensor de movimientos / Cámaras de vigilancia / Sistema de alarmas / Chapa y cerrajería 5. Establecer procedimiento para el control de cambios de contraseña 6. Procedimiento evaluación de capacidad, desempeño y obsolecencia tecnológica del sistema. 7. Implementar zonas de exclusión y controles de seguridad física	01/09/2021	01/09/2022	- MAE - Direcciones de Área y Direcciones Administrativas. - Personal de Sistemas de planta o consultores. - RSI	1. Actualización, mantenimiento del generador electricidad para garantizar niveles mínimos de servicio 2. Adquisición de UPS para protección de Equipos Sensibles
5	*Controles criptográficos para la protección de la información*	1. PISI 8.10 2. PISI 8.9 3. PISI 9 - 8.8 Inciso e)	1. Política y procedimiento para controles criptográficos. - Implementar algoritmos de encripatacion para envio y recepcion de informacion critica y	01/09/2021	01/09/2022	- Personal de Sistemas de planta o consultores. - RSI - Jefe Nacional de Asuntos Jurídicos FC – BCB	Capacitación al personal de la enidad respecto a seguridad de información

N°	ACTIVO DE INFORMACIÓN PRIORIZADO	CONTROLES A IMPLEMENTARSE	ACCIONES A DESARROLLAR	FECHA DE INICIO	FECHA DE CONCLUSIÓN	RESPONSABLES	REQUERIMIENTO PARA LA IMPLEMENTACIÓN DE LA ACCIÓN
			confidencial . 2. Política y procedimiento para el control de accesos. 3. Implementar un reglamento para la sancion y medidas disciplinarias para usuarios que incumplan la PSI				
6	***Protección de archivos de soporte digital o fisico***	1. - PISI 8.8 - PISI 8.9 - PISI 8.12 - PISI 8.13 inciso f) - PISI 8.15 - PISI 8.16 2. PISI 8.8 Inciso e)	1. - Política y procedimientos para el manejo de información clasificada - Implementar mecanismos para la protección y resguardo de información clasificada. - Implementar políticas para digitalización de documentación física para una óptima seguridad y disponibilidad de la misma. - Procedimiento de prueba de medios de respaldo (backups) 2. Implementar un reglamento para la sanción y medidas disciplinarias para usuarios que incumplan la PSI	01/09/2021	01/09/2022	- Personal de Sistemas de planta o consultores. - RSI - Jefe Nacional de Asuntos Jurídicos FC - BCB	Capacitación al personal de la entidad respecto a seguridad de información
7	***Acceso remoto a equipos de oficina para desarrollo de actividades de modalidad Teletrabajo***	- PISI 8.12 - PISI 8.13 - PISI 8.14 - PISI 8.15 - PISI 8.16	1. Implementar una política y un procedimiento para contingencias tecnológicas. 2. "Implementación de UPS." 3. Implementación de cronograma de mantenimiento Implementación de cronograma de actualización	01/09/2021	01/09/2022	- Personal de Sistemas de planta o consultores. - RSI - Jefe Nacional de Asuntos Jurídicos FC - BCB	Capacitación al personal de la entidad respecto a seguridad de información

Fuente: Elaboración Propia

ANEXO I – CATÁTOLO DE AMENAZAS SEGÚN MAGERIT VERSIÓN 3.0

[N] Desastres Naturales

Natural (accidental)

[N.1] Fuego	
Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware)	1. [D] disponibilidad
• [Media] soportes de información	
• [AUX] equipamiento auxiliar	
• [L] instalaciones	
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. Ver: EBIOS: 01- INCENDIO	

[I] Desastres Industriales

[I.5] Avería de origen físico o lógico

[I.5] Avería de origen físico o lógico	
Tipos de activos:	Dimensiones:
• [SW] aplicaciones (software)	1. [D] disponibilidad
• [Media] soportes de información	
• [AUX] equipamiento auxiliar	
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante. Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 28 - AVERÍA DEL HARDWARE 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE	

[I.6] Corte del suministro eléctrico

[I.6] Corte del suministro eléctrico	
Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware)	1. [D] disponibilidad
• [Media] soportes de información (electrónicos)	
• [AUX] equipamiento auxiliar	

Descripción: cese de la alimentación de potencia Origen: Entorno (accidental) Humano (accidental o deliberado) Ver: EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA

[A.] Accesos

[A.11] Acceso no autorizado

[A.11] Acceso no autorizado	
Tipos de activos:	Dimensiones:
• [D] datos / información	1. [C] confidencialidad 2. [I] integridad
• [keys] claves criptográficas	
• [S] servicios	
• [SW] aplicaciones (software)	
• [HW] equipos informáticos (hardware)	
• [COM] redes de comunicaciones	
• [Media] soportes de información	
• [AUX] equipamiento auxiliar	
• [L] instalaciones	
Descripción: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. Ver: EBIOS: 33 - USO ILÍCITO DEL HARDWARE	

[A.12] Análisis de tráfico

[A.12] Análisis de tráfico	
Tipos de activos:	Dimensiones:
• [COM] redes de comunicaciones	1. [C] confidencialidad
Descripción: el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico". Ver: EBIOS: no disponible	

[A.15] Modificación deliberada de la información

[A.15] Modificación deliberada de la información	
Tipos de activos:	Dimensiones:
• [D] datos / información	
• [keys] claves criptográficas	

• [S] servicios (acceso)	1. [D] disponibilidad
• [SW] aplicaciones (SW)	
• [COM] comunicaciones (tránsito)	
• [Media] soportes de información	
• [L] instalaciones	
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Ver: EBIOS: no disponible	

[A.18] Destrucción de información

[A.18] Destrucción de información	
Tipos de activos:	Dimensiones:
• [D] datos / información	1. [D] disponibilidad
• [keys] claves criptográficas	
• [S] servicios (acceso)	
• [SW] aplicaciones (SW)	
• [Media] soportes de información	
• [L] instalaciones	
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. Ver: EBIOS: 01- INCENDIO	

[E] Errores

[E.1] Errores de los usuarios

E.1] Errores de los usuarios	
Tipos de activos:	Dimensiones:
• [D] datos / información	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
• [keys] claves criptográficas	
• [S] servicios	
• [SW] aplicaciones (software)	
• [Media] soportes de información	
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. Ver: EBIOS: 38 - ERROR DE USO	

[E.2] Errores del administrador

[E.2] Errores del administrador	
Tipos de activos:	Dimensiones:
• [D] datos / información	
• [keys] claves criptográficas	

• [S] servicios	1. [D] disponibilidad
• [SW] aplicaciones (software)	2. [I] integridad
• [HW] equipos informáticos (hardware)	3. [C] confidencialidad
• [COM] redes de comunicaciones	
• [Media] soportes de información	
Descripción: equivocaciones de personas con responsabilidades de instalación, mantenimiento y/o operación Ver: EBIOS: 38 - ERROR DE USO	

[E.3] Errores de monitorización (log)

[E.3] Errores de monitorización (log)	
Tipos de activos:	Dimensiones:
• [D.log] registros de actividad	1. [I] integridad (trazabilidad)
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos. Ver: EBIOS: no disponible	

[E.4] Errores de configuración

[E.4] Errores de configuración	
Tipos de activos:	Dimensiones:
• [D.conf] datos de configuración	1. [I] integridad
Descripción: introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Ver: EBIOS: no disponible	

[E.7] Deficiencias en la organización

[E.7] Deficiencias en la organización	
Tipos de activos:	Dimensiones:
• [P] personal	1. [D] disponibilidad
Descripción: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc. Ver: EBIOS: no disponible	

[E.8] Difusión de software dañino

[E.8] Difusión de software dañino

Tipos de activos:	Dimensiones:
• [SW] aplicaciones (software)	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. Ver: EBIOS: no disponible	

[E.14] Escapes de información

[E.14] Escapes de información	
Tipos de activos:	Dimensiones:
•	1. [C] confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

[E.15] Alteración accidental de la información

E.15] Alteración accidental de la información	
Tipos de activos:	Dimensiones:
• [D] datos / información	1. [I] integridad
• [keys] claves criptográficas	
• [S] servicios	
• [SW] aplicaciones (SW)	
• [COM] comunicaciones (tránsito)	
• [Media] soportes de información	
• [L] instalaciones	
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Ver: EBIOS: no disponible	

[E.19] Fugas de información

[E.19] Fugas de información	
Tipos de activos:	Dimensiones:
• [D] datos / información	
• [keys] claves criptográficas	
• [S] servicios	

• [SW] aplicaciones (SW)	1. [C] confidencialidad
• [COM] comunicaciones (tránsito)	
• [Media] soportes de información	
• [L] instalaciones	
• [P] personal (revelación)	
Descripción: introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Ver: EBIOS: no disponible	

[E.20] Vulnerabilidades de los programas (software)

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos:	Dimensiones:
• [SW] aplicaciones (software)	1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. Ver: EBIOS: no disponible	

[E.21] Errores de mantenimiento / actualización de programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos:	Dimensiones:
• [SW] aplicaciones (software)	1. [I] integridad 2. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. Ver: EBIOS: 31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware)	1. [D] disponibilidad
• [Media] soportes electrónicos	
• [AUX] equipamiento auxiliar	
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. Ver: EBIOS: 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN	

[E.24] Caída del sistema por agotamiento de recursos

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos:	Dimensiones:
• [S] servicios	1. [D] disponibilidad
• [HW] equipos informáticos (hardware)	
• [COM] redes de comunicaciones	
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Ver: EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	

[E.25] Pérdida de equipos

[E.25] Robo	
Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware)	1. [D] disponibilidad 2. [C] confidencialidad
• [Media] soportes de información	
• [AUX] equipamiento auxiliar	
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. Ver: EBIOS: 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS	

[E.28] Indisponibilidad del personal

[E.28] Indisponibilidad del personal	
Tipos de activos:	Dimensiones:
• [P] personal interno	1. [D] disponibilidad

Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ... Ver: EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL

[A] Ataques intencionados

[A.3] Manipulación de los registros de actividad (log)

[A.3] Manipulación de los registros de actividad (log)	
Tipos de activos:	Dimensiones:
• [D.log] registros de actividad	1. [I] integridad (trazabilidad)
Descripción: Ver: EBIOS: no disponible	

[A.4] Manipulación de la configuración

[A.4] Manipulación de la configuración	
Tipos de activos:	Dimensiones:
• [D.log] registros de actividad	1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Ver: EBIOS: no disponible	

[A.5] Suplantación de la identidad del usuario

[A.5] Suplantación de la identidad del usuario	
Tipos de activos:	Dimensiones:
• [D] datos / información	1. [C] confidencialidad 2. [A] autenticidad 3. [I] integridad
• [keys] claves criptográficas	
• [S] servicios	
• [SW] aplicaciones (software)	
• [COM] redes de comunicaciones	

Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. Ver: EBIOS: 40 - USURPACIÓN DE DERECHO

[A.6] Abuso de privilegios de acceso

[A.6] Abuso de privilegios de acceso	
Tipos de activos:	Dimensiones:
• [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. Ver: EBIOS: 39 - ABUSO DE DERECHO	

[A.7] Uso no previsto

[A.7] Uso no previsto	
Tipos de activos:	Dimensiones:
• [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	1. [D] disponibilidad 2. [C] confidencialidad 3. [I] integridad

Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. Ver: EBIOS: no disponible

[A.4] Manipulación de la configuración

[A.4] Manipulación de la configuración	
Tipos de activos:	Dimensiones:
• [D.log] registros de actividad	1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Ver: EBIOS: no disponible	

[A.9] [Re-]encaminamiento de mensajes

[A.9] [Re-]encaminamiento de mensajes	
Tipos de activos:	Dimensiones:
• [S] servicios	1. [C] confidencialidad
• [SW] aplicaciones (software)	
• [COM] redes de comunicaciones	
Descripción: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe. Ver: EBIOS: no disponible	

[A.11] Acceso no autorizado

[A.11] Acceso no autorizado	
Tipos de activos:	Dimensiones:
• [D] datos / información	1. [C] confidencialidad
• [keys] claves criptográficas	
• [S] servicios	
• [SW] aplicaciones (software)	

• [HW] equipos informáticos (hardware)	2. [I] integridad
• [COM] redes de comunicaciones	
• [Media] soportes de información	
• [AUX] equipamiento auxiliar	
• [L] instalaciones	
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. Ver: EBIOS: 33 - USO ILÍCITO DEL HARDWARE	

[A.12] Análisis de tráfico

[A.12] Análisis de tráfico	
Tipos de activos:	Dimensiones:
• [D.log] registros de actividad	1. [I] integridad 2. [C] confidencialidad 3. [A] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Ver: EBIOS: no disponible	

[A.23] Manipulación de los equipos

[A.23] Manipulación de los equipos	
Tipos de activos:	Dimensiones:
• [HW] equipos	
• [Media] soportes de información	1. [C] confidencialidad
• [AUX] equipamiento auxiliar	2. [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. Ver: EBIOS: 25 - SABOTAJE DEL HARDWARE	

[A.24] Denegación de servicio

[A.24] Denegación de servicio	
Tipos de activos:	Dimensiones:
• [S] servicios	
• [HW] equipos informáticos (hardware)	1. [D] disponibilidad
• [COM] redes de comunicaciones	

Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Ver: EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO

[A.25] Robo

[A.25] Robo	
Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware)	
• [Media] soportes de información	1. [D] disponibilidad
• [AUX] equipamiento auxiliar	2. [C] confidencialidad
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. Ver: EBIOS: 20 - ROBO DE SOPORTES O DOCUMENTOS 21 - ROBO DE HARDWARE	

[A.30] Ingeniería social (picaresca)

[A.30] Ingeniería social (picaresca)	
Tipos de activos:	
• [P] personal interno	1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. Ver: EBIOS: no disponible	

[BMSC.1] Denegación de Servicio ICBanking

[BMSC.1] Denegación de Servicio ICBanking	
Tipos de activos:	Dimensiones:
• [S] Perdida del Servicio de Banca por Internet ICBanking	1. [D] disponibilidad
Descripción: Bloqueos en la Datos del Sistema ICBanking provocada por proccesos de depuracion de tablas de Log´s. Ver: GRIST 2015 - 02	

[BMSC.2] Perdida de Servicio OnBase

[BMSC.2] Perdida de Servicio OnBase, plataforma de ventas, sistema de corrspondencia, EDV, ACH y pago de servicios MC4 a través de FISA.	
Tipos de activos:	Dimensiones:
• [SL] Lentitud en el servicio por consumo de recursos	1. [D] disponibilidad
Descripción: Perdida de servicio con Onbase, plataforma de ventas, sistema de correspondencia, EDV, ACH y pago de servicios a MC4 a traves de FISA. Por procesos indexados (Onbase), transacciones ACH, pago de servicios, envio de infomación a EDV. Por actualización de certificados. Ver: GRIST 2015 - 01	

[BMSC.3] Lentitud en el acceso a maquina virtual

[BMSC.3] Lentitud en el acceso a maquina virtual del servidor On Base	
Tipos de activos:	Dimensiones:
• [MV] Maquina Virtual	1. [D] disponibilidad
Descripción: No disponibilidad de cliente Web del sistema OnBase. Ver: GRIST 2 - 2014	

[A.30] Ingeniería social (picaresca)

[A.30] Ingeniería social (picaresca)	
Tipos de activos:	Dimensiones:
• [P] personal interno	1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. Ver: EBIOS: no disponible	

[BMSC.4] Apps en repositorios de terceros

[BMSC.4] Apps en repositorios de terceros

Tipos de activos:	Dimensiones:
• [App] Publicaciones de ipa y apk	1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad
Descripción: Los usuarios pueden visitar y descargar apps desde tiendas de terceros que pueden alojar aplicaciones maliciosas. El riesgo se presenta cuando las aplicaciones del BMSC no se obtienen de la tienda oficial. Ver: 31000 RIESGOS	

ANEXO II - GENERALIZACIÓN DE ACTIVOS DE LA INFORMACIÓN

NRO.	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	UBICACIÓN	UNIDAD RESPONSABLE	CUSTODIO
1	E1	UPS	Para la gestión de energía regulada	Equipamiento Auxiliar	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
2	H1	DELL EMC PowerEdge R740	Procesador Dos (2) x Intel Xeon Gold 6136 3.0G, 12C/24T, 10.4GT/s , 24.75M Cache, Turbo, HT (150W) DDR4-2666, RAM 256 GB, HDD 30 TB, Tarjeta de Red Broadcom 57416 2 Port 10Gb Base-T + 5720 2 Port 1Gb Base-T, rNDC	Hardware	Sección de Sistemas / Fundación Cultural del Banco Central de Bolivia (FC-BCB)	Unidad Nacional de Administración y Finanzas	Técnico Informático
3	H2	Ares	Intel Xeon E5320 1.86 GHz 2 GB 70 GB. Windows Server 2012 R2	Hardware	Biblioteca Pública / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Biblioteca Pública	Jefe de Administración y finanzas

NRO.	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	UBICACIÓN	UNIDAD RESPONSABLE	CUSTODIO
4	H3	Cerbero	Hp Proliant ML 350 G6 Intel Xeon E5620 2.40 GHz 12 GB 2.5 teras. Windows Server 2008 R2	Hardware	Área de digitalización / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Dirección	Digitalizador
5	H4	DELL R820	Intel Xeon procesador E5-4600	Hardware	Administración / Casa Nacional de la Moneda (CNM)	Administración	Profesional en Sistemas
6	H5	Dell Storage NX3230	DELL, Intel Xeon E5-2630 v3 2.4GHz, 32GB RAM, Discos(2x300GB) SAS , (10x 4TB NLSAS) Red: Broadcom 5720 QP 1Gb	Hardware	Sección Sistemas / Museo Nacional de Etnografía y Folklore (MUSEF)	Administración y Finanzas	Informático

NRO.	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	UBICACIÓN	UNIDAD RESPONSABLE	CUSTODIO
7	H6	Equipos de Escritorio	DELL, HP, MAC, Toshiba, Sony, equipos de escritorio de todas las dependencias de la Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Hardware	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	Usuarios
8	H7	Firewall	- Firewall Pfsense. - Firewall Watguard - Juniper SSG5, SRX100 - MICROTIK RB2011UiAS-2HnD V.6.42.7 - Sophos SG230	Hardware	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	

NRO.	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	UBICACIÓN	UNIDAD RESPONSABLE	CUSTODIO
9	H8	HADES	HP ProLiant ML350 G5. Windows Server 2008 R2, Intel® Xeon E5420 @ 2.5 GHz(8 CPUs), 2,5GHz 4096 MB RAM, 64 BITS, 279,36 GB.	Hardware	Área de digitalización / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Dirección	Digitalizador
10	H9	HP	Procesador Intel Core 2Duo CPU 2.92Ghz, Memoria RAM 2,00GB, Disco C 2,46GB, Disco D 151GB. Para el Sistema Visual de Contabilidad y SIGA de Almacén, Windows 7 Profesional	Hardware	Administración y Finanzas / Centro de la cultura Plurinacional (CCP)	Administración y Finanzas	Jefe Unidad De Administración y Finanzas

NRO.	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	UBICACIÓN	UNIDAD RESPONSABLE	CUSTODIO
11	H10	Impresoras	Impresoras de todas las dependencias de la Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Hardware	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
12	H11	Nemesis	HP Proliant ML 150 G6 Intel Xeon E5504 2.40 GHz 12GB 2 TB. Windows Server 2016	Hardware	Área de digitalización / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Dirección	Digitalizador
13	H12	PC-A	HP(vISUAL)	Hardware	Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Administración	Asistente contable
14	H13	PC-DB	HP Pro 3500 MT, I5 650 3.20GHz, 4 GB RAM, 1 TERA. Windows 7	Hardware	Área de digitalización / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Dirección	Digitalizador

NRO.	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	UBICACIÓN	UNIDAD RESPONSABLE	CUSTODIO
15	H14	Poweredge R530	Dell, Intel® Xeon® E5-2600 V3 2.4ghz, Ram 16 Gb, Hdd 2 Tb.	Hardware	Administración y Finanzas / Casa de la Libertad (CDL)	Administración y Finanzas	Personal de apoyo Sistemas
16	H15	PowerEdge VRTX	DELL Procesador: Intel Xeon E5-2660 2.20GHz, 2 Procesadores de la misma capacidad, 32GB RAM, Discos y 3 cuchillas	Hardware	Sección Sistemas / Museo Nacional de Etnografía y Folklore (MUSEF)	Administración y Finanzas	Informático
17	H16	Prometeo	HP ProLiant ML110 G7 Intel® Xeon E31220 @ 3.10 GHz(8 CPUs), 2,5GHz 6GiB RAM. Ubuntu 10,01,4 LTS	Hardware	Área de digitalización / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Dirección	Digitalizador
18	H17	Servervisualfinal	2 Gb Ram, 500 Gb Hdd, 2 Procesadores (Numa, Sockets)	Hardware	Administración y Finanzas / Casa de la Libertad (CDL)	Administración y Finanzas	Personal de apoyo Sistemas

NRO.	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	UBICACIÓN	UNIDAD RESPONSABLE	CUSTODIO
19	H18	Servidor Dell POWEREDGE R230	Servidor Tipo Rack Marca: Dell, Modelo: Poweredge R230, Serie: Cn-05401-10g00-830-00be-A01, Color: Negro	Hardware	Sala de Monitoreo / Museo Nacional de Arte (MNA)	*Unidad Administrativo Financiero*	*Portero – MNA*
20	H19	Servidor Rack POWEREDGE730	Servidor Tipo Rack Chasis Disco De 2.5 Pulgadas Procesador Intel Xeon 32 Ghz Con Lector Dvd "Dell" Modelo: Poweredge730	Hardware	Sala de Monitoreo / Museo Nacional de Arte (MNA)	*Unidad Administrativo Financiero*	*Portero – MNA*
21	H20	Storage A	Storage Qnap Ts-12353u	Hardware	Administración / Casa Nacional de la Moneda (CNM)	Administración	Profesional en Sistemas
22	H21	Storage B	Power vault MD3620i 10x 400gb ssd 10x1.2gb	Hardware	Sección Sistemas / Museo Nacional de Etnografía y Folklore (MUSEF)	Administración y Finanzas	Informático

NRO.	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	UBICACIÓN	UNIDAD RESPONSABLE	CUSTODIO
			Power vault MD1200 10x4 TB SAS Power vault MD1200 12x6 TB SAS Power vault MD1200 10X8 TB SAS				
23	H22	Switch	DELL N4032 administrable 24 puertos	Hardware	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Administración y Finanzas	
24	H23	Telefonía	Central Telefónica Gadstream, Central Digital Ip Con Elissa, Xorcom	Hardware	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
25	I1	Almacenamiento	Openfiler	Información	PowerEdge VRTX / Museo Nacional de Etnografía y Folklore (MUSEF)	Administración y Finanzas	Usuarios

NRO.	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	UBICACIÓN	UNIDAD RESPONSABLE	CUSTODIO
26	P1	Personal	Funcionarios Públicos	Personal	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
27	RC1	Internet	Internet Entel ADSL y FIBRA, AXS	Redes de Comunicaciones	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
28	RC2	VPN	VPN SIGMA, VPN FCBCB	Redes de Comunicaciones	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	

29	S1	Zimbra	Correo electrónico	Servicios	PowerEdge VRTX / Museo Nacional de Etnografía y Folklore (MUSEF)	Administración y Finanzas	Usuarios
30	S2	ABCD	Sistema de gestión Bibliotecaria, para el procesamiento técnico de material bibliográfico y servicios bibliotecarios.	Servicios	HADES / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Dirección	Digitalizador
31	S3	BibArch	Sistema para el registro de investigadores, solicitudes de documentos y control de Servicios brindados en Sala de investigaciones del ABNB	Servicios	PC-DB / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Dirección	Digitalizador
32	S4	Página web	Dell R820, RAM 16gb, HDD 80 GB, LINUX/Ubuntu 14	Servicios	Servidor Dell R820 / Casa Nacional de la Moneda (CNM)	Administración	Profesional en Sistemas
33	S5	Servidor DNS , Página electrónica	Página web, servidor dns	Servicios	PowerEdge VRTX / Museo Nacional de Etnografía y Folklore (MUSEF)	Administración y Finanzas	Usuarios

34	S6	Servidor web (Web hosting)	RAM 2GB, HDD 5GB, LINUX/CENTOS7, MySQL, PHP	Servicios	Servidor Externo / Fundación Cultural del Banco Central de Bolivia (FC-BCB)	Unidad Nacional de Administración y Finanzas	Técnico Informático
35	S7	Sistema de biblioteca koha	Sistema de Biblioteca integrado Koha	Servicios	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
36	S8	Spark	Sistema de Mensajería	Servicios	Sala del Servidor / Fundación Cultural del Banco Central de Bolivia (FC-BCB)	Unidad Nacional de Administración y Finanzas	Técnico Informático
37	SA1	Antivirus	Antivirus	Software	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
38	SA2	Atom (Sistema de Catalogación de Archivo)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	Servidor Dell R821 / Casa Nacional de la Moneda (CNM)	Administración	Profesional en Sistemas

39	SA3	Biométrico	Control de Asistencia Biométrico	Software	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
40	SA4	Biostar2	Procesador Dos (2) x Intel Xeon Gold 6136 2.99 Ghz, RAM 8 GB, HDD 250 GB, Windows Server 2012	Software	Sala del Servidor / Fundación Cultural del Banco Central de Bolivia (FC-BCB)	Unidad Nacional de Administración y Finanzas	Técnico en Recursos Humanos
41	SA5	Contabilidad Visual	Programa integrado de información financiera, para elaborar estados Contables, Presupuestarios y otros	Software	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
42	SA6	DigiArch	Sistema de gestión archivística, para el registro de la descripción archivística de documentos.	Software	CERBERO / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Dirección	Digitalizador

43	SA7	E-Control	Laptop Toshiba, 3.6 Ghz, RAM 12 GB, HDD 1TB, Windows 10	Software	Recursos Humanos / Fundación Cultural del Banco Central de Bolivia (FC-BCB)	Unidad Nacional de Administración y Finanzas	Técnico en Recursos Humanos
44	SA8	Ofimática	Aplicaciones Word, Excel, Powerpoint, etc.	Software	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
45	SA9	Registro Inventario	Sistema para el registro de ingreso de documentos en la Unidad de Archivo del ABNB, en base al formato RBC2 de la FCBCB	Software	PC-DB / Archivo y Biblioteca Nacionales de Bolivia (ABNB)	Dirección	Digitalizador
46	SA10	Siga	Sistema Almacenes	Software	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	

47	SA11	Sigamos Portable	Aplicación DE ESCRITORIO Que Permite Generar Reportes Personalizados de Los Movimientos Del Almacén	Software	Poweredge R531 / Casa de la Libertad (CDL)	Administración y Finanzas	Personal de apoyo Sistemas
48	SA12	Sistema de Administración de Libros (SIALI)	Sistema para donación, venta, intercambio de libros	Software	PowerEdge VRTX / Museo Nacional de Etnografía y Folklore (MUSEF)	Administración y Finanzas	Informático
49	SA13	Sistema de Bienes Culturales	Administración y catalogación de bienes culturales	Software	POWEREDGE732 / Museo Nacional de Arte (MNA)	Unidad Administrativo Financiero	Jefe De Unidad De Administración y Finanzas
50	SA14	Sistema de contrataciones	Genera, almacena e imprime los formularios de los bienes y servicios	Software	POWEREDGE731 / Museo Nacional de Arte (MNA)	Unidad Administrativo Financiero	Jefe De Unidad De Administración y Finanzas
51	SA15	Sistema de correspondencia	Sistema para el manejo, y derivar la correspondencia	Software	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	

52	SA16	Sistema de museo	Sistema de catalogación de bienes museográficos	Software	PowerEdge VRTX / Museo Nacional de Etnografía y Folklore (MUSEF)	Administración y Finanzas	Informático
53	SA17	Sistema Operativo Servidor	Debian GNU/Linux. Red Hat Linux. Ubuntu Linux. Microsoft Windows Server 2003 Standard, Microsoft Windows Server 2008 (64-bit), Centos Linux Windows Server 2016 Windows 7	Software	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	
54	SA18	Sistema Operativo usuario	Sistema operativo en computadores de escritorio Windows 7, 8,10	Software	Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Unidad Nacional de Administración y Finanzas	Usuario
55	SA19	Sistema S.I.A (Sistema Integrado de Archivo)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	Servidor Dell R825 / Casa Nacional de la Moneda (CNM)	Administración	Profesional en Sistemas

56	SA20	Sistema S.I.C (Sistema Integrado de Catalogación)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	Servidor Dell R824 / Casa Nacional de la Moneda (CNM)	Administración	Profesional en Sistemas
57	SA21	Sistema S.I.C (Sistema Integrado de Corte)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	Servidor Dell R826 / Casa Nacional de la Moneda (CNM)	Administración	Profesional en Sistemas
58	SA22	Sistema S.I.R (Sistema Integrado de Requerimientos)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	Servidor Dell R823 / Casa Nacional de la Moneda (CNM)	Administración	Profesional en Sistemas
59	SI1	Plataforma de Virtualización Microsoft Hyper-V Server	VM # 1 : Windows Xp Sql-Server - Servidor de Contabilidad Visual	Soporte de la información	Servidor Servervisualfinal / Casa de la Libertad (CDL)	Administración y Finanzas	Personal de apoyo Sistemas
60	SI2	Plataforma de Virtualización Proxmox VE	MV # 1 : Windows server r2 2012 - Acceso controlado a servicios de red MV # 2 : Windows server r2 2008 - Acceso controlado a servicios del sistema visual contable MV # 3 : Ubuntu	Soporte de la información	Dell R820 / Casa Nacional de la Moneda (CNM)	Administración	Profesional en Sistemas

			14 - Página web - Sistema S.I.A - Sistema S.I.C . MV # 4 : Ubuntu 16 - Sistema atom MV # 5 : Ubuntu 16 - Sistema koha MV # 6 : ubuntu 16 - Compartidos MV # 7 : ubuntu 16 - Servidor FTP				
61	SI3	Plataforma de Virtualización VMWARE ESXI	VM # 1: Windows Server 2008R2 – Contabilidad Visual VM # 2: Centos7 - Servidor Web VM # 3: Centos7 - Servidor DNS VM# 4: Centos7 – Almacenes VM # 5: Debian10 – Agenda Cultural VM # 6: Windows Server 2012R2 – Biométrico	Soporte de la información	DELL EMC PowerEdge R740 / Fundación Cultural del Banco Central de Bolivia (FC-BCB)	Unidad Nacional de Administración y Finanzas	Técnico Informático

			VM # 7: Windows Server 2012R2 – Antivirus VM # 8: Centos7 – Correo Institucional VM # 9: Centos7 – Spark VM # 10: Ubuntu14 – Correspondencia				
62	SI4	Plataforma de Virtualización VMware vSphere	MV # 1 : Debian 10 - Página web, DNS MV # 2: Centos 7 - Sistema almacenes, Correspondencia, marcado virtual. MV # 3: Centos 4 - DNS Server MV # 4 : Debian 10 - Koha MV # 5 : Openfiler - Almacenamiento MV # 6 : Windows server 2003 -	Soporte de la información	PowerEdge VRTX / Museo Nacional de Etnografía y Folklore (MUSEF)	Administración y Finanzas	Informático

			Sistema De museología MV # 7 : Red Hat - Sistema de biblioteca MV # 8 : Ubuntu - AtoM MV # 9 : Linux - Servidor NAS				

ANEXO III VALORACIÓN DE ACTIVOS DE INFORMACIÓN

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
1	E1	UPS	Para la gestión de energía regulada	Equipamiento Auxiliar	5	1	2	8	
2	H1	DELL EMC PowerEdge R740	Procesador Dos (2) x Intel Xeon Gold 6136 3.0G, 12C/24T, 10.4GT/s , 24.75M Cache, Turbo, HT (150W) DDR4-2666, RAM 256 GB, HDD 30 TB, Tarjeta de Red Broadcom 57416 2 Port 10Gb Base-T + 5720 2 Port 1Gb Base-T, rNDC	Hardware	5	4	5	14	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
3	H2	Ares	Intel Xeon E5320 1.86 GHz 2 GB 70 GB. Windows Server 2012 R2	Hardware	5	4	5	14	
4	H3	Cerbero	Hp Proliant ML 350 G6 Intel Xeon E5620 2.40 GHz 12 GB 2.5 teras. Windows Server 2008 R2	Hardware	5	4	5	14	
5	H4	DELL R820	Intel Xeon procesador E5-4600	Hardware	5	4	5	14	
6	H5	Dell Storage NX3230	DELL, Intel Xeon E5-2630 v3 2.4GHz, 32GB RAM, Discos(2x300GB) SAS , (10x 4TB NLSAS) Red: Broadcom 5720 QP 1Gb	Hardware	5	4	5	14	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
7	H6	Equipos de Escritorio	DELL, HP, MAC, Toshiba, Sony, equipos de escritorio de todas las dependencias de la Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Hardware	5	5	4	14	
8	H7	Firewall	- Firewall Pfsense. - Firewall Watguard - Juniper SSG5, SRX100 - MICROTIK RB2011UiAS-2HnD V.6.42.7 - Sophos SG230	Hardware	4	3	4	11	
9	H8	HADES	HP ProLiant ML350 G5. Windows Server 2008 R2, Intel® Xeon E5420 @ 2.5 GHz(8 CPUs), 2,5GHz 4096 MB RAM, 64 BITS, 279,36 GB.	Hardware	5	4	5	14	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
10	H9	HP	Procesador Intel Core 2Duo CPU 2.92Ghz, Memoria RAM 2,00GB, Disco C 2,46GB, Disco D 151GB. Para el Sistema Visual de Contabilidad y SIGA de Almacén, Windows 7 Profesional	Hardware	5	4	5	14	
11	H10	Impresoras	Impresoras de todas las dependencias de la Fundación Cultural del Banco Central de Bolivia (FC-BCB), Repositorios Nacionales y Centros Culturales	Hardware	1	2	2	5	
12	H11	Nemesis	HP Proliant ML 150 G6 Intel Xeon E5504 2.40 GHz 12GB 2 TB. Windows Server 2016	Hardware	5	4	5	14	
13	H12	PC-A	HP(vISUAL)	Hardware	5	4	5	14	
14	H13	PC-DB	HP Pro 3500 MT, I5 650 3.20GHz, 4 GB RAM, 1 TERA. Windows 7	Hardware	5	4	5	14	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
15	H14	Poweredge R530	Dell, Intel® Xeon® E5-2600 V3 2.4ghz, Ram 16 Gb, Hdd 2 Tb.	Hardware	5	4	5	14	
16	H15	PowerEdge VRTX	DELL Procesador: Intel Xeon E5-2660 2.20GHz, 2 Procesadores de la misma capacidad, 32GB RAM, Discos y 3 cuchillas	Hardware	5	4	5	14	
17	H16	Prometeo	HP ProLiant ML110 G7 Intel® Xeon E31220 @ 3.10 GHz(8 CPUs), 2,5GHz 6GiB RAM. Ubuntu 10,01,4 LTS	Hardware	5	4	5	14	
18	H17	Servervisualfinal	2 Gb Ram, 500 Gb Hdd, 2 Procesadores (Numa, Sockets)	Hardware	5	4	5	14	
19	H18	Servidor Dell POWEREDGE R230	Servidor Tipo Rack Marca: Dell, Modelo: Poweredge R230, Serie: Cn-05401-10g00-830-00be-A01, Color: Negro	Hardware	5	4	5	14	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
20	H19	Servidor Rack POWEREDGE 730	Servidor Tipo Rack Chasis Disco De 2.5 Pulgadas Procesador Intel Xeon 32 Ghz Con Lector Dvd "Dell" Modelo: Poweredge730	Hardware	5	4	5	14	
21	H20	Storage A	Storage Qnap Ts-12353u	Hardware	5	4	5	14	
22	H21	Storage B	Power vault MD1200 10x4 tb SAS Power vault MD1200 12x6 tb SAS Power vault MD3620i 10x 400gb ssd 10x1.2gb	Hardware	5	4	5	14	
23	H22	Switch	DELL N4032 administrable 24 puertos	Hardware	5	5	5	15	
24	H23	Telefonía	Central Telefónica Gadstream, Central Digital Ip Con Elissa, Xorcom	Hardware	1	2	1	4	
25	I1	Almacenamiento	Openfiler	Información	5	4	5	14	
26	P1	Personal	Funcionarios Públicos	Personal	5	4	5	14	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
27	RC1	Internet	Internet Entel ADSL y FIBRA, AXS	Redes de Comunicaciones	3	3	2	8	
28	RC2	VPN	VPN SIGMA, VPN FCBCB	Redes de Comunicaciones	3	3	2	8	
29	S1	Zimbra	correo electrónico	Servicios	1	1	2	4	
30	S2	ABCD	Sistema de gestión Bibliotecaria, para el procesamiento técnico de material bibliográfico y servicios bibliotecarios.	Servicios	2	2	2	6	
31	S3	BibArch	Sistema para el registro de investigadores, solicitudes de documentos y control de Servicios brindados en Sala de investigaciones del ABNB	Servicios	2	2	2	6	
32	S4	Pagina web	Dell R820, RAM 16gb, HDD 80 GB, LINUX/Ubuntu 14	Servicios	2	2	2	6	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
33	S5	Servidor DNS , Página electrónica	Página web, servidor dns	Servicios	2	2	3	7	
34	S6	Servidor web (Web hosting)	RAM 2GB, HDD 5GB, LINUX/CENTOS7, MySQL, PHP	Servicios	2	2	3	7	
35	S7	Sistema de biblioteca koha	Sistema de Biblioteca integrado Koha	Servicios	2	2	2	6	
36	S8	Spark	Sistema de Mensajería	Servicios	1	1	3	1	
37	SA1	Antivirus	Antivirus	Software	3	2	3	8	
38	SA2	Atom (Sistema de Catalogación de Archivo)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	2	2	2	6	
39	SA3	Biométrico	Control de Asistencia Biométrico	Software	5	3	4	12	
40	SA4	Biostar2	Procesador Dos (2) x Intel Xeon Gold 6136 2.99 Ghz, RAM 8 GB, HDD 250 GB, Windows Server 2012	Software	5	3	4	12	
41	SA5	Contabilidad Visual	Programa integrado de información financiera, para elaborar estados Contables,	Software	5	3	4	12	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
			Presupuestarios y otros						
42	SA6	DigiArch	Sistema de gestión archivística, para el registro de la descripción archivística de documentos.	Software	2	2	2	6	
43	SA7	E-Control	Laptop Toshiba, 3.6 Ghz, RAM 12 GB, HDD 1TB, Windows 10	Software	5	3	4	12	
44	SA8	Ofimática	Aplicaciones Word, Excel, Powerpoint, etc.	Software	5	3	4	12	
45	SA9	Registro Inventario	Sistema para el registro de ingreso de documentos en la Unidad de Archivo del ABNB, en base al formato RBC2 de la FCBCB	Software	5	4	3	12	
46	SA10	Siga	Sistema Almacenes	Software	5	4	3	12	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
47	SA11	Sigamos Portable	Aplicación DE ESCRITORIO Que Permite Generar Reportes Personalizados de Los Movimientos Del Almacén	Software	5	4	3	12	
48	SA12	Sistema de Administración de Libros(SIALI)	Sistema para donación, venta, intercambio de libros	Software	5	4	3	12	
49	SA13	Sistema de Bienes Culturales	Administración y catalogación de bienes culturales	Software	5	4	3	12	
50	SA14	Sistema de contrataciones	Genera, almacena e imprime los formularios de los bienes y servicios	Software	5	4	3	12	
51	SA15	Sistema de correspondencia	Sistema para el manejo, y derivar la correspondencia	Software	2	2	4	8	
52	SA16	Sistema de museo	Sistema de catalogación de bienes museográficos	Software	5	4	3	12	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
53	SA17	Sistema Operativo Servidor	Debian GNU/Linux. Red Hat Linux. Ubuntu Linux. Microsoft Windows Server 2003 Standard, Microsoft Windows Server 2008 (64-bit), Centos Linux Windows Server 2016 Windows 7	Software	5	4	3	12	
54	SA18	Sistema Operativo usuario	Sistema operativo en computadores de escritorio Windows 7, 8,10	Software	4	2	3	9	
55	SA19	Sistema S.I.A (Sistema Integrado de Archivo)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	5	4	3	12	
56	SA20	Sistema S.I.C (Sistema Integrado de Catalogación)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	5	4	3	12	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
57	SA21	Sistema S.I.C (Sistema Integrado de Corte)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	5	4	3	12	
58	SA22	Sistema S.I.R (Sistema Integrado de Requerimientos)	Dell R820, RAM 8gb, HDD 80 GB, LINUX/Ubuntu 16	Software	5	4	3	12	
59	SI1	Plataforma de Virtualización Microsoft Hyper-V Server	VM # 1 : Windows Xp Sql-Server - Servidor de Contabilidad Visual	Soporte de la información	5	4	3	12	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
60	SI2	Plataforma de Virtualización Proxmox VE	MV # 1 : Windows server r2 2012 - Acceso controlado a servicios de red MV # 2 : Windows server r2 2008 - Acceso controlado a servicios del sistema visual contable MV # 3 : Ubuntu 14 - Página web - Sistema S.I.A - Sistema S.I.C MV # 4 : Ubuntu 16 - Sistema atom MV # 5 : Ubuntu 16 - Sistema koha MV # 6 : ubuntu 16 - Compartidos MV # 7 : ubuntu 16 - Servidor FTP	Soporte de la información	5	4	3	12	
61	SI3	Plataforma de Virtualización VMWARE ESXI	VM # 1: Windows Server 2008R2 – Contabilidad Visual VM # 2: Centos7 - Servidor Web	Soporte de la información	5	4	3	12	

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
			VM # 3: Centos7 - Servidor DNS VM# 4: Centos7 – Almacenes VM # 5: Debian10 – Agenda Cultural VM # 6: Windows Server 2012R2 – Biométrico VM # 7: Windows Server 2012R2 – Antivirus VM # 8: Centos7 – Correo Institucional VM # 9: Centos7 – Spark VM # 10: Ubuntu14 – Correspondencia					

NRO	CÓDIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	TIPOS DE ACTIVO	VALORACIÓN DE ACTIVOS			VALORACIÓN FINAL	FECHA DE INICIO
					Disponibilidad	Integridad	Confidencialidad		
62	SI4	Plataforma de Virtualización VMware vSphere	MV # 1 : Ubuntu 14 - Página web, DNS MV # 2 : Windows server r2 2008 - Sistema de Libros MV # 3 : Windows server 2003 - Sistema De museología MV # 4 : Ubuntu 14 - zimbra MV # 5 : Ubuntu 16 - Sistema Almacenes MV # 6 : Openfiler - Almacenamiento MV # 7 : Red Hat - Sistema de biblioteca MV # 7 : Debian - Koha	Soporte de la información	5	4	3	12	

ANEXO IV IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DE RIESGOS

N°	Activo/Proceso	Amenaza	Situación	Vulnerabilidad	VALORACIÓN DE ACTIVOS			RIESGO			
					D	I	C	Valoración de riesgo	Probabilidad	Impacto	Nivel del Riesgo
1	Sistemas de Correspondencia	- Deficiencias en la organización - Vulnerabilidades del programa, se puede Hackear el sistema. - Fue creado para uso provisional. - Varios repositorios no cuentan con el sistema.	- No hay control para el sistema. - Se debe acudir a ayuda externa de la ADSIB. - Es aceptable porque el registro se realiza con sumo cuidado, haciendo una revisión constante de todos los datos ingresados.	- Defecto de software, debido a que nos es posible hacer seguimiento a algunos procesos y no se puede realizar buenos backups. - Ausencia de Documentación.	1	1	3	1,67	Muy probable	Severo	Alto

N°	Activo/Proceso	Amenaza	Situación	Vulnerabilidad	VALORACIÓN DE ACTIVOS				RIESGO		
					D	I	C	Valoración de riesgo	Probabilidad	Impacto	Nivel del Riesgo
2	Sistema de Recursos Humanos Biometrico	- Corte de suministro eléctrico prolongado. - Errores, manipulación de configuración. - Abuso de privilegios de acceso. - Modificación deliberada de la información, al hacer cambios no autorizados en la marcación de asistencia.	- El equipo biométrico tiene en su interior una batería de respaldo de energía de 4 horas, no cuenta con UPS. - Implicaciones legales, proceso interno	- Asignación erradade los derechos de acceso. - Ausencia de control de cambios eficaz - Falta de conciencia acerca de la seguridad	2	2	2	2,00	Probable	Menor	**Bajo**
3	Internet ADSL - Fibra	- Corte de suministro electrico. - Fallo de servicios de comunicaciones. - Errores de configuración - Abuso de privilegios de acceso	- Equipos de red tienes UPS de suministro electrico - Servicio deficiente. Proceso internos o implicaciones legales por el mal uso y la falta de control.	- Vulnerabilidades de red, corte de servicio. - Servicio Deficiente. - Ausencia de políticas para el uso de los medios de telecomunicaciones.	2	2	1	1,67	Probable	Moderado	**Medio**

N°	Activo/Proceso	Amenaza	Situación	Vulnerabilidad	VALORACIÓN DE ACTIVOS				RIESGO		
					D	I	C	Valoración de riesgo	Probabilidad	Impacto	Nivel del Riesgo
4	Registro de Boletas de Licencia y Vacación	- Errores de mantenimiento / actualización de programas (software). - Avería de origen físico o lógico. - Uso no previsto, equipo de computación y Software de Asistencia en la misma PC. Vulnerabilidades de los programas (software), no ayuda a realizar las tareas de manera mecánica y a reducir tiempos del procedimiento de registros. - Error del administrador.	- Se realiza el backup de la base de datos del software de asistencia (una vez cada mes), también se tiene varias copias de seguridad del software de asistencia en discos. - Registro de asistencia deficinete con ausencia de vacaciones y licencias.	- Configuración por defecto. - Vulnerabilidades del programa	2	2	2	2,00	Probable	Menor	**Bajo**

N°	Activo/Proceso	Amenaza	Situación	Vulnerabilidad	VALORACIÓN DE ACTIVOS				RIESGO		
					D	I	C	Valoración de riesgo	Probabilidad	Impacto	Nivel del Riesgo
5	Mantenimiento de sistemas de información	- Deficiencias en la organización Ausencia o insuficiencia de control de calidad.	- Revisión básica de los sistemas de acuerdo a la falla detectada.	- Sistemas de información con defectos de calidad. - Modificación accidental de componentes del sistema.	2	2	3	2,33	Muy probable	Moderado	**Alto**
6	Equipo de computación	- Deficiencias en la organización, ausencia de Personal técnico calificado en Sistemas. - Corte de suministro eléctrico - Difusión de software dañino, falla de equipos por virus. - Errores de mantenimiento / actualización de	- Algunos equipos no cuentan con UPS. - Sin copias de seguridad y mantenimiento de los equipos de computacion. - Algunos equipos no cuentan con Antivirus.	- Falla de funcionamiento de hardware. - Falla de funcionamiento de software. - Código malicioso	3	2	2	2,33	Probable	Moderado	**Medio**

N°	Activo/Proceso	Amenaza	Situación	Vulnerabilidad	VALORACIÓN DE ACTIVOS				RIESGO		
					D	I	C	Valoración de riesgo	Probabilidad	Impacto	Nivel del Riesgo
		equipos (hardware) - Avería del hardware.									
7	Firewall	- Denegación de servicio. - Corte de suministro electrico. - Errores de mantenimiento / actualización software	- Carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	- Interrupción de servicios. - Fallas de hardware o software	3	2	2	2,33	Probable	Moderado	**Medio**
8	Sistema Integral de Gestión de Almacenes (SIGA)	- Deficiencias en la organización - Vulnerabilidades del programa.	- No permite generar reportes personalizados de los movimientos del Almacén.	- Fallo de la red eléctrica	3	2	3	2,67	Probable	Moderado	**Medio**

N°	Activo/Proceso	Amenaza	Situación	Vulnerabilidad	VALORACIÓN DE ACTIVOS				RIESGO		
					D	I	C	Valoración de riesgo	Probabilidad	Impacto	Nivel del Riesgo
9	Contabilidad Visual	- Difusión de software dañino	Sensible a cambios de configuración en el servidor central.	- Almacenamiento sin protección. - Ausencia de un eficiente control de cambios en la configuración.	3	2	3	2,67	Probable	Severo	**Alto**
10	Servidores	-Avería de origen físico o lógico. - Falla de funcionamiento de hardware. - Falla de equipos auxiliares de suministro eléctrico. - Falta de aterramiento en sistema eléctrico. - Falta de piso técnico para servidores. - Falta de sistema de refrigeración.		- Suceptibilidad a las variaciones de temperatura. - Suceptibilidad a la humedad, el plvo y la suciedad. - Red energética inestable. - Ausencia de protección física de la edificación, puertas y ventanas. - Uso inadecuado o descuidado del control de acceso físico a las instalaciones.	3	3	3	3,00	Cierta/Inminente	Crítico	**Crítico**

N°	Activo/Proceso	Amenaza	Situación	Vulnerabilidad	VALORACIÓN DE ACTIVOS				RIESGO		
					D	I	C	Valoración de riesgo	Probabilidad	Impacto	Nivel del Riesgo
11	Controles Criptográficos para la protección de la información	- Acceso no autorizado - Modificación deliberada de la información - Destrucción de información. - Fugas de información	No se utiliza controles criptograficos	- Violación de accesos - Arquitectura insegura - Entrenamiento insuficiente en seguridad.	2	2	2	2,00	Muy probable	Crítico	**Crítico**
12	Protección de archivos de soporte digital ó físico, respaldos, documentos, credenciales de acceso y otros	- Pérdida accidental de la información. - Escapes de información. - Fugas de información.	Sin procedimiento de manejo de Archivos.	-Almacenamiento sin protección. - Tablas de contraseñas sin protección	3	2	2	2,33	Cierta/Inminente	Crítico	**Crítico**
13	Acceso remoto a equipos de oficina para desarrollo de actividades de modalidad Teletrabajo	- Inestabilidad de conexión de internet - Perdida de información	Sin procedimientos para acceso remoto	- Uso no controlado de acceso a los equipos	5	4	3	4	Muy Probable	Severo	**Alto**

ANEXO V CONTROL DE CRITICIDAD DE ACTIVOS DE INFORMACIÓN INSTITUCIONAL PRIORIZADOS

Activo:	Sistema de Correspondencia	Nivel Riesgo Actual
ID:		16
Tipo:	SOFTWARE	Nivel Riesgo Residual
Valor del activo:	8	6

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Acceso no autorizado	La falta de mecanismos de identificación y autenticación de usuarios, como ser (Login, Password, Tokens, Tarjetas, Aplicaciones.) / Carencia de procedimientos para el acceso a sistemas de información	Control de accesos mediante login y password	4	4	16	Ato	PISI 8.14 PISI 8.16 PISI 8.9	Implementación de procedimientos para el control de altas, bajas y modificación de los derechos de acceso.	1	4	4	Bajo
Acceso no autorizado	Deficiente gestión de contraseñas	Inexistente	4	4	16	Ato	PISI 8.14 PISI 8.16 PISI 8.9	Procedimiento para el control de cambios de contraseña	1	4	4	Bajo

Activo:	Sistema de Correspondencia	Nivel Riesgo Actual
ID:		16
Tipo:	SOFTWARE	Nivel Riesgo Residual
Valor del activo:	8	6

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Denegación de Servicio	Falta de actualización del sistema / Desorden de documentos en la organización / No genera el correlativo de la gestión que sigue por lo que hay que crear otra base de datos. / Deficiencia de varias opciones para el seguimiento de acciones administrativas	Inexistente	4	4	16	Alto	PISI 8.14 PISI 8.16 PISI 8.9	Implementar un procedimiento actualización del sistema y/o reemplazar el sistema	2	4	8	Medio

Activo:	Sistema de Correspondencia	Nivel Riesgo Actual
ID:		16
Tipo:	SOFTWARE	Nivel Riesgo Residual
Valor del activo:	8	6

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Monitoreo de tráfico	No se cuenta con un programa de análisis de vulnerabilidad	Inexistente	4	4	16	Alto	PISI 8.14 PISI 8.16 PISI 8.9	Implementación de procedimientos para el análisis y gestión de vulnerabilidades técnicas / realización de pruebas de Ethical Hacking.	2	4	8	Medio
Saturación / Desempeño deficiente	Obsolecencia plataforma tecnologica	Inexistente	4	4	16	Alto	PISI 8.14 PISI 8.16 PISI 8.9	Procedimiento de evaluación de obsolecencia	2	4	8	Medio
Cyber Amenazas	Carencia de un proceso de desarrollo seguro	Inexistente	4	4	16	Alto	PISI 8.14 PISI 8.16 PISI 8.9	Implementacion de procedimientos para la ingenieria y desarrollo de software	1	4	4	Bajo
Cyber Amenazas	Carencia de requerimientos de seguridad	Inexistente	4	4	16	Alto	PISI 8.14 PISI 8.16 PISI 8.9	Implementar una política y un	1	4	4	Bajo

Activo:	Sistema de Correspondencia	Nivel Riesgo Actual
ID:		16
Tipo:	SOFTWARE	Nivel Riesgo Residual
Valor del activo:	8	6

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
								procedimiento para contingencias tecnológicas.				
Total					112		Total				40	
Total de Riesgo Actual (R/7)					16		Total de Riesgo Actual (R/7)				6	

Activo:	Mantenimiento de sistemas de información	Nivel Riesgo Actual
ID:		12
Tipo:	SOFTWARE	Nivel Riesgo Residual
Valor del activo:	6	4

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Acceso no autorizado	Asignación errónea de los derechos de acceso	No se cuenta con controles al respecto	2	4	8	Alto	PISI 8.14	Implementacion de politicas y procedimientos de seguridad para el control de derechos de acceso a Bases de Datos	1	4	4	Bajo
Divulgación de información	No se cuenta con un programa de análisis de vulnerabilidad	Inexistente	4	4	16	Alto	PISI 8.14	Implementación de procedimientos para el análisis y gestión de vulnerabilidades técnicas.	1	4	4	Bajo
Ataques por vulnerabilidades	Alteración de cambio de información por falta de seguridad	inexistente	3	4	12	Alto	PISI 8.8 PISI 8.14	Implementación de procedimientos para la revisión periódica de las politicas de seguridad	1	4	4	Bajo

Activo:	Mantenimiento de sistemas de información	Nivel Riesgo Actual
ID:		12
Tipo:	SOFTWARE	Nivel Riesgo Residual
Valor del activo:	6	4

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Perdida información	Carencia de archivos de respaldo para información sensible	Se cuenta con backup periodico / No se cuenta con procedimientos formal	3	4	12	Alto	PISI 8.12	Implementación de Procedimientos para la gestión de Backups	2	4	8	Medio
Código malicioso	Modificación de información por falta de actualización de antivirus	Inexistente	3	4	12	Alto	PISI 8.13	Implementación de software libre (Antivirus)	1	2	2	Muy bajo
Total					60		Total				22	
Total de Riesgo Actual (R/5)					12		Total de Riesgo Residual (R/5)				4	

Activo:	Sistema de Contabilidad Visual : SQLServer	Nivel Riesgo Actual
ID:		12
Tipo:	SOFTWARE	Nivel Riesgo Residual
Valor del activo:	6	6

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Acceso no autorizado	Asignación errónea de los derechos de acceso	No se cuenta con controles al respecto	3	4	12	Alto	PISI 8.14 PISI 8.16 PISI 8.15	Implementacion de politicas y procedimientos de seguridad para el control de derechos de acceso a Bases de Datos	1	4	4	Bajo
Monitoreo de tráfico	No se cuenta con un programa de análisis de vulnerabilidad	Inexistente	3	4	12	Alto	PISI 8.14 PISI 8.16 PISI 8.15	Implementación de procedimientos para el análisis y gestión de vulnerabilidades técnicas / realización de pruebas de Ethical Hacking	1	4	4	Bajo

Activo:	Sistema de Contabilidad Visual : SQLServer	Nivel Riesgo Actual
ID:		12
Tipo:	SOFTWARE	Nivel Riesgo Residual
Valor del activo:	6	6

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Fraude / Robo	Ausencia de registros de auditoría ("logs") de los administradores y operadores	Inexistente	3	4	12	Alto	PISI 8.14 PISI 8.16 PISI 8.15	Implementación de procedimientos para la revisión periódica de Pistas de Auditoría / Implementación de Pistas de Auditoría	1	4	4	Bajo
Perdida información	Carencia de archivos de respaldo para información sensible	Se cuenta con backup periodico / No se cuenta con procedimientos adecuados	3	4	12	Alto	PISI 8.14 PISI 8.16 PISI 8.15	Implementación de Procedimientos para la gestión de Backups	1	4	4	Bajo
Fallas de hardware	Sistemas en equipos de computación	Inexistente	3	4	12	Alto	PISI 8.14 PISI 8.16 PISI 8.15	Implementación de Procedimientos para la adquisición de equipos para el Sistema	3	4	12	Alto

Activo:	Sistema de Contabilidad Visual : SQLServer	Nivel Riesgo Actual
ID:		12
Tipo:	SOFTWARE	Nivel Riesgo Residual
Valor del activo:	6	6

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Total					60		Total				28	
Total de Riesgo Actual (R/5)					12		Total de Riesgo Actual (R/5)				6	

Activo:	Servidores	Nivel Riesgo Actual
ID:		25
Tipo:	HARDWARE	Nivel Riesgo Residual
Valor del activo:	7	16

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado (PISI)	Actividades	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Condiciones ambientales adversas	Sensibilidad a la humedad, polvo, suciedad	Inexistente	5	5	25	Crítico	PISI 8.11 PISI 8.13 PISI 8.9 PISI 8.12	Adaptacion del ambiente, sistemas de alarma, extintores entre otros.	5	5	25	Crítico
Condiciones ambientales adversas	Sensibilidad a la radiación electromagnética	No se cuenta con controles al respecto	5	5	25	Crítico	PISI 8.11 PISI 8.13 PISI 8.9 PISI 8.12	- Implementacion de aterramiento electrico. - Implementacion de acometida electrica.	5	5	25	Crítico
suministro de energia y equipos de continuidad electrica	Sensibilidad a variaciones de tensión / Fuente de alimentación Inestable	componentes de energia UPS	5	5	25	Crítico	PISI 8.11 PISI 8.13 PISI 8.9 PISI 8.12	Implementacion de UPS.	5	5	25	Critico

Activo:	Servidores	Nivel Riesgo Actual
ID:		25
Tipo:	HARDWARE	Nivel Riesgo Residual
Valor del activo:	7	16

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado (PISI)	Actividades	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Condiciones ambientales adversas	Sensibilidad a la temperatura	No se cuenta con aire acondicionado y sensores de humo	5	5	25	Crítico	PISI 8.11 PISI 8.13 PISI 8.9 PISI 8.12	Implementacion de aire acondicionado de presicion	5	5	25	Crítico
Falla del hardware	Mantenimiento deficiente	Se cuenta con mantenimiento correctivo y preventivo	5	5	25	Crítico	PISI 8.11 PISI 8.13 PISI 8.9 PISI 8.12	Implementacion de cronograma de mantenimiento	1	2	2	Muy Bajo
Falla del hardware	Único punto de error (falta de dispositivos de contingencia)	Se realiza mantenimiento correctivo	5	5	25	Crítico	PISI 8.11 PISI 8.13 PISI 8.9 PISI 8.12	- Implementacion de Plan de Contingencia	1	2	2	Muy Bajo
Robo o pérdida del hardware	Deficiencias en el resguardo y proteccion del activo	El control se encuentra en una zona de exclusion	5	5	25	Crítico	PISI 8.11 PISI 8.13 PISI 8.9 PISI 8.12	Implementacion de acceso biometrico, camaras de vigilancia y detector de movimiento	5	5	25	Crítico

Activo:	Servidores	Nivel Riesgo Actual
ID:		25
Tipo:	HARDWARE	Nivel Riesgo Residual
Valor del activo:	7	16

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado (PISI)	Actividades	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Acceso no autorizado	Deficiente gestión de contraseñas	Inexistente	5	5	25	Crítico	PISI 8.11 PISI 8.13 PISI 8.9 PISI 8.12	Procedimiento para el control de cambios de contraseña Criptografías	1	2	2	Muy Bajo
Total					200		Total				131	
Total de Riesgo Actual (R/8)					25		Total de Riesgo Actual (R/8)				16	

Activo:	Controles criptográficos para la protección de la información	Nivel Riesgo Actual
ID:		20
Tipo:	INF. DIGITAL	Nivel Riesgo Residual
Valor del activo:	5	9

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividades	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Acceso no Autorizado	La falta de procedimientos y herramientas para la clasificación y protección de información	Inexistente	4	5	20	Crítico	PISI 8.10 PISI 8.9 PSII 8.8	Implementar un procedimiento específico para clasificación de información	1	5	5	Bajo
Divulgación	Copias no controladas de documentos confidenciales	Inexistente	4	5	20	Crítico	PISI 8.10 PISI 8.9 PSII 8.8	Política y procedimiento para el control de accesos.	1	5	5	Bajo
Perdida información	Fallas de medio de almacenamiento	Inexistente	4	5	20	Crítico	PISI 8.10 PISI 8.9 PSII 8.8	Procedimiento para el resguardo de Información en repositorio	1	5	5	Bajo

Activo:	**Controles criptográficos para la protección de la información**	**Nivel Riesgo Actual**										
ID:		20										
Tipo:	**INF. DIGITAL**	**Nivel Riesgo Residual**										
Valor del activo:	5	9										

Amenaza	**Vulnerabilidad**	**Control Existente**	**Riesgo Actual**				**Control recomendado**		**Riesgo Residual**			
			P	**I**	**R**	**NR**		**Actividades**	**P**	**I**	**R**	**NR**
Robo y Fraude	Deficiencias en el resguardo y proteccion del activo	Inexistente	4	5	20	Crítico	PISI 8.10 PISI 8.9 PSII 8.8	Implementar el control de acceso biométrico / cerrajes magnéticos / Zonas de Exclusión	4	5	20	Crítico
Total					80		**Total**				35	
Total de Riesgo Actual (R/4)					20		**Total de Riesgo Actual (R/4)**				9	

Activo:	Protección de archivos de soporte digital o físico	Nivel Riesgo Actual
ID:		25
Tipo:	INF. DIGITAL	Nivel Riesgo Residual
Valor del activo:	5	10

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Acceso no Autorizado	La falta de procedimientos y herramientas para la clasificación y protección de información	inexistente	5	5	25	Critico	PISI 8.12 PISI 8.13 PISI 8.15 PISI 8.16 PISI 8.9 PSII 8.8	Implementar un procedimiento específico para clasificación de información	1	5	5	Bajo
Divulgación	Copias no controladas de documentos confidenciales	inexistente	5	5	25	Critico	PISI 8.12 PISI 8.13 PISI 8.15 PISI 8.16 PISI 8.9 PSII 8.8	Implementar mecanismos para la protección y resguardo de información clasificada	1	5	5	Bajo
Perdida información	Fallas de medio de almacenamiento	Se cuenta backup actualizado	5	5	25	Critico	PISI 8.12 PISI 8.13 PISI 8.15 PISI 8.16 PISI 8.9 PSII 8.8	Capacitación al personal de la entidad respecto a seguridad de información	1	5	5	Bajo

Activo:	Protección de archivos de soporte digital o físico	Nivel Riesgo Actual
ID:		25
Tipo:	INF. DIGITAL	Nivel Riesgo Residual
Valor del activo:	5	10

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Robo y Fraude	Deficiencias en el resguardo y proteccion del activo	Zona de exclusión, cerrajes , camaras , sensores de seguridad fisica	5	5	25	Critico	PISI 8.12 PISI 8.13 PISI 8.15 PISI 8.16 PISI 8.9 PSII 8.8	Implementar Control de acceso biométrico / cerrajes magnéticos / Zonas de Exclusión	5	5	25	Critico
Total					100		Total				40	
Total de Riesgo Actual (R/4)					25		Total de Riesgo Actual (R/4)				10	

Activo:	Acceso remoto a equipos de oficina para desarrollo de actividades de modalidad Teletrabajo	Nivel Riesgo Actual
ID:		15
Tipo:	INF. DIGITAL	Nivel Riesgo Residual
Valor del activo:	4	5

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Fallo de servicios de comunicaciones	Sin acceso a internet	Inexistente	4	4	16	Alto	PISI 8.12 PISI 8.13	Implementar una política y un procedimiento para contingencias tecnológicas.	2	2	4	Bajo
Interrupción de otros servicios y suministros esenciales	Fallas en el sistema eléctrico	Inexistente	4	4	16	Alto	PISI 8.12	Implementacion de UPS.	2	2	4	Bajo

Activo:	Acceso remoto a equipos de oficina para desarrollo de actividades de modalidad Teletrabajo	Nivel Riesgo Actual	
ID:		15	
Tipo:	INF. DIGITAL	Nivel Riesgo Residual	
Valor del activo:	4	5	

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Errores de mantenimiento / actualización de equipos (hardware)	Falta de mantenimento físico.		4	4	16	Alto	PISI 8.14 PISI 8.16	Implementación de cronograma de mantenimento	2	2	4	Bajo
Errores de mantenimiento / actualización de programas (software)	Falta de herramientas de actualización		4	4	16	Alto	PISI 8.14 PISI 8.16	Implementación de cronograma de actualización	2	1	2	Irrelevante

Activo:	Acceso remoto a equipos de oficina para desarrollo de actividades de modalidad Teletrabajo	Nivel Riesgo Actual
ID:		15
Tipo:	INF. DIGITAL	Nivel Riesgo Residual
Valor del activo:	4	5

Amenaza	Vulnerabilidad	Control Existente	Riesgo Actual				Control recomendado	Actividad	Riesgo Residual			
			P	I	R	NR			P	I	R	NR
Alteración accidental de la información	La falta de procedimientos y herramientas para la clasificación y protección de información	Básico	3	3	9	Medio	PISI 8.15	En proceso de implementación según normativa vigentente	3	3	9	Medio
Total					73		Total					23
Total de Riesgo Actual (R/5)					15		Total de Riesgo Residual (R/4)					5