RESOLUCIÓN ADMINISTRATIVA N.° 0057/2026
GERENCIA GENERAL

ASUNTO: DESIGNACIÓN DEL RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (RSI), CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI) Y APROBACIÓN DE LA ACTUALIZACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI) – GESTIÓN 2026

HR: I/2026-01705
FECHA: 13 de agosto de 2026

VISTOS:

El Informe Técnico **INF/GG/USI/FCC/2026-00037**, de fecha 10 de agosto de 2026, emitido por el Área de Sistemas y Nuevas Tecnologías de la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil – EBC; el documento denominado **Actualización "Plan Institucional de Seguridad de la Información "**, identificado con código **EBC-USNT-PL-00001, Versión N.° 2.1**; el Memorándum **MEM/GG/SMS/2026-00013**, de fecha 14 de julio de 2026; el Informe Legal **INF/GG/UJ/BASR/2026-00052** de fecha 12 de agosto de 2026correspondiente; la Resolución Administrativa EBC N.° 0157/2023 de 26 de octubre de 2023; el Decreto Supremo N.° 1020, de 26 de octubre de 2011; la Ley N.° 164, de 8 de agosto de 2011; el Decreto Supremo N.° 1793, de 13 de noviembre de 2013; el Decreto Supremo N.° 2514, de 9 de septiembre de 2015, modificado por el Decreto Supremo N.° 5519, de 13 de enero de 2026; la Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, modificada por la Resolución Administrativa AGETIC/RA/0059/2018, de 1 de agosto de 2018; el Comunicado OFEP/DGE/SER N.° 015/2026, de 29 de junio de 2026; la Nota Externa AGETIC/NE/1466/2026, de 10 de junio de 2026; el Informe Técnico AGETIC-CGII/IT/0067/2026, de 10 de junio de 2026; y demás antecedentes administrativos y técnicos que forman parte del expediente.

CONSIDERANDO I:

Que, el parágrafo II del artículo 103 de la Constitución Política del Estado establece que el Estado asumirá como política la implementación de estrategias

www.ebc.gob.bo
Av. Brasil N° 1636 Zona Miraflores, La Paz-Bolivia
Email: ebcbolivia@ebc.gob.bo
Telf.: (591-2)-2188100

para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.

Que, el artículo 232 de la Constitución Política del Estado establece que la Administración Pública se rige por los principios de legitimidad, legalidad, imparcialidad, publicidad, compromiso e interés social, ética, transparencia, igualdad, competencia, eficiencia, calidad, calidez, honestidad, responsabilidad y resultados.

Que, los numerales 1 y 2 del artículo 235 de la Constitución Política del Estado establecen como obligaciones de las servidoras y los servidores públicos cumplir la Constitución y las leyes y asumir las responsabilidades inherentes al ejercicio de la función pública.

Que, el artículo 71 de la Ley N.º 164, de 8 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, declara de prioridad nacional la promoción del uso de las tecnologías de información y comunicación para procurar el vivir bien de las bolivianas y los bolivianos.

Que, el parágrafo I del artículo 72 de la Ley N.º 164 dispone que el Estado fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, incluyendo la seguridad informática y de redes; asimismo, el artículo 75 establece que el nivel central del Estado promoverá la incorporación del Gobierno Electrónico a los procedimientos gubernamentales y a la prestación de sus servicios.

Que, el artículo 8 del Decreto Supremo N.º 1793, de 13 de noviembre de 2013, dispone que las entidades públicas promoverán la seguridad informática para la protección de los datos en sus sistemas informáticos, mediante planes de contingencia desarrollados e implementados en cada entidad.

Que, el Decreto Supremo N.º 2514, de 9 de septiembre de 2015, creó la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC y estableció competencias relacionadas con el Gobierno Electrónico y la seguridad de la información en las entidades del sector público.

Que, el Decreto Supremo N.º 5519, de 13 de enero de 2026, modificó el artículo 17 del Decreto Supremo N.º 2514, estableciendo que las entidades del sector público deben desarrollar e implementar el Plan Institucional de Seguridad de la

Información – PISI conforme a los lineamientos establecidos por el Centro de Gestión de Incidentes Informáticos – CGII.

Que, asimismo, el Decreto Supremo N.º 5519 modificó el parágrafo II del artículo 18 del Decreto Supremo N.º 2514, disponiendo que las entidades del sector público deben designar al Responsable de Gobierno Electrónico y Tecnologías de Información y Comunicación y al Responsable de Seguridad de la Información, a fin de coordinar con la AGETIC.

Que, mediante Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, se aprobaron los "Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público", modificados posteriormente por la Resolución Administrativa AGETIC/RA/0059/2018, de 1 de agosto de 2018.

Que, el punto 6.1.2 de los citados Lineamientos establece la designación y funciones del Responsable de Seguridad de la Información – RSI, quien tiene la responsabilidad de coadyuvar en la elaboración, implementación, seguimiento y mejora del PISI.

Que, el punto 6.1.3 de los Lineamientos PISI establece que, mediante resolución administrativa o resolución expresa, según corresponda, la Máxima Autoridad Ejecutiva designará al personal que conformará el Comité de Seguridad de la Información – CSI, de acuerdo con el tamaño de la estructura organizativa, volumen y complejidad de las operaciones de la entidad.

Que, conforme al mismo punto 6.1.3, el CSI estará conformado por la Máxima Autoridad Ejecutiva en calidad de Presidente, personal de nivel jerárquico de acuerdo con la estructura organizativa de la entidad y el Responsable de Seguridad de la Información – RSI, correspondiéndole, entre otras funciones, revisar el PISI, promover su aprobación ante la MAE, revisar los procedimientos de seguridad, proponer estrategias para el fortalecimiento de controles y efectuar el seguimiento de indicadores y métricas de seguridad de la información.

Que, el punto 6.4 de los Lineamientos PISI establece que el Plan Institucional de Seguridad de la Información debe ser revisado por el Comité de Seguridad de la Información – CSI, instancia que impulsará su aprobación ante la Máxima Autoridad Ejecutiva.

UNIDAD JURÍDICA V°B° C.R.A.M. EBC

UNIDAD JURÍDICA V°B° R.D.C. EBC

CONSIDERANDO II:

Que, mediante Informe Tecnico **INF/GG/USI/FCC/2026-00037**, de fecha 10 de agosto de 2026, el Área de Sistemas y Nuevas Tecnologías de la EBC solicitó la revisión y aprobación del documento denominado **"Actualización Plan Institucional de Seguridad de la Información "**, código **EBC-USNT-PL-00001, Versión N.° 2.1**, así como la emisión de la correspondiente Resolución Administrativa de Gerencia General.
Que, de los antecedentes remitidos se establece que la EBC cuenta con un Plan Institucional de Seguridad de la Información aprobado mediante **Resolución Administrativa EBC N.° 0157/2023, de 26 de octubre de 2023**, constituyéndose dicho instrumento en el marco interno para la gestión y protección de la información institucional.

Que, durante la gestión 2026, la Oficina Técnica para el Fortalecimiento de la Empresa Pública – OFEP, en coordinación con AGETIC, emitió el **Comunicado OFEP/DGE/SER N.° 015/2026, de 29 de junio de 2026**, relativo a la regularización del cumplimiento de las medidas de control y protección de la información, implementación del PISI y acreditación del Sistema de Gestión de Seguridad de la Información en las empresas públicas.

Que, asimismo, constituyen antecedentes técnicos de la actualización y regularización del PISI la **Nota Externa AGETIC/NE/1466/2026** y el **Informe Técnico AGETIC-CGII/IT/0067/2026**, ambos de fecha 10 de junio de 2026.

Que, en atención a los antecedentes y disposiciones señaladas, el Área de Sistemas y Nuevas Tecnologías de la EBC procedió a revisar y actualizar el PISI institucional, incorporando ajustes normativos y técnicos, formalización del Responsable de Seguridad de la Información – RSI, actualización del inventario y clasificación de la información institucional, matriz de reporte por eje estratégico y cronograma de regularización correspondiente a la gestión 2026.

Que, la actualización presentada mantiene la estructura general del PISI aprobado anteriormente e incorpora, entre otros, los siguientes elementos: actualización del marco normativo; formalización del RSI; actualización del inventario y clasificación de la información institucional; incorporación de matriz de reporte por eje estratégico; cronograma de regularización y actualización correspondiente a la gestión 2026; incorporación de los Anexos V y VI;

actualización del control de cambios; e identificación del documento como **Versión N.° 2.1**.

Que, conforme al Informe Técnico citado, se propone formalizar la designación del servidor público **Félix Chambi Conde**, Técnico II en Sistemas y Nuevas Tecnologías, dependiente del Área de Sistemas y Nuevas Tecnologías, como **Responsable de Seguridad de la Información – RSI titular de la EBC**, designación que cuenta como antecedente con el Memorándum **MEM/GG/SMS/2026-00013, de fecha 14 de julio de 2026**.

Que, en consecuencia, corresponde formalizar mediante Resolución Administrativa la designación del Responsable de Seguridad de la Información – RSI, en observancia del Decreto Supremo N.° 2514, modificado por el Decreto Supremo N.° 5519, y de los Lineamientos PISI emitidos por AGETIC.

RESPONSABLE SEGÚN D.S. N° 2514	
DESIGNACION COMO:	**NOMBRE Y APELLIDO**
Responsable de Seguridad de la Información (RSI)	Ing. Félix Chambi Conde

Que, asimismo, corresponde conformar el Comité de Seguridad de la Información – CSI de la EBC, como instancia institucional encargada de revisar el PISI, promover su aprobación, efectuar seguimiento a su implementación y contribuir al fortalecimiento de la seguridad de la información institucional.

DESIGNACION DEL COMITÉ DE SEGURIDAD DE LA INFORMACION (CSI)		
COMITÉ DE SEGURIDAD	**NOMBRES Y APELLIDOS**	**CARGO DEL FUNCIONARIO**
Presidente del CSI	Ing. Sergio Mustafá Sáenz	Gerente General
Miembro del CSI	Lic. María Aleja Peñaranda Tapia	Gerente Aaministrativo Financiero
Miembro del CSI	Ing. Wilson Campero Laruta	Jefe Unidad de Planificación y Gestión de Calidad.
Miembro del CSI	Dra. Cecilia Aparicio Molina	Responsable de la Unidad Jurídica
Miembro del CSI	Ing. Félix Chambi Conde	Responsable del Area de Sistemas y Nuevas tecnologías

Que, el artículo 8 del Decreto Supremo N.° 1020, de 26 de octubre de 2011, establece que la EBC está a cargo de un Gerente General, quien se constituye en su Máxima Autoridad Ejecutiva y define los asuntos de su competencia mediante resoluciones administrativas.

Que, el numeral 4 del artículo 9 del Decreto Supremo N.° 1020 establece como función del Gerente General aprobar los Reglamentos y Manuales que

UNIDAD JURIDICA V°B° C.R.A.M. EBC

UNIDAD JURIDICA V°B° B.A.R.D.C. EBC

correspondan, mientras que el numeral 6 del mismo artículo le atribuye la función de diseñar e implementar sistemas de gestión institucional que incluyan reglamentos, metodologías y procedimientos necesarios para la ejecución, monitoreo, seguimiento, supervisión y evaluación de las actividades de la Empresa.

Que, por tanto, corresponde al Gerente General, en su condición de Máxima Autoridad Ejecutiva de la EBC, aprobar la actualización del Plan Institucional de Seguridad de la Información – PISI, Gestión 2026, y disponer las medidas necesarias para su implementación.

CONSIDERANDO III

Que, de la revisión técnica y jurídica efectuada, se establece que el documento denominado **Actualizacion Plan Institucional de Seguridad de la Información** código **EBC-USNT-PL-00001**, **Versión N.º 2.1**, incorpora elementos compatibles con los Lineamientos PISI, entre ellos el inventario y clasificación de activos de información, metodología de gestión de riesgos, controles, indicadores, gestión de incidentes, contingencias tecnológicas, cronograma de implementación y mecanismos de seguimiento y mejora continua.

Que, la actualización del PISI no constituye la creación de un instrumento institucional desvinculado del Plan anterior, sino la actualización de la versión vigente, correspondiendo identificarla como **Versión N.º 2.1 – Gestión 2026**, por lo que resulta necesario evitar la coexistencia de versiones institucionales contradictorias.

Que, en consecuencia, corresponde dejar sin efecto la Resolución Administrativa EBC N.º 0157/2023, de 26 de octubre de 2023, **únicamente en cuanto a la aprobación del PISI anterior**, entrando en vigencia el nuevo instrumento aprobado mediante la presente Resolución Administrativa.

Que, mediante Informe Legal correspondiente, la Unidad Jurídica de la EBC estableció que la actualización del PISI, la designación del RSI y la conformación del CSI cuentan con sustento técnico y jurídico suficiente y no contravienen el ordenamiento jurídico vigente, recomendando su aprobación mediante Resolución Administrativa de Gerencia General.

POR TANTO:

El Gerente General de la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil – EBC, en ejercicio de las atribuciones conferidas por el Decreto Supremo N.° 1020, de 26 de octubre de 2011, la normativa vigente y demás disposiciones aplicables,

RESUELVE:

ARTÍCULO PRIMERO.- APROBAR el documento denominado **ACTUALIZACION DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN – ACTUALIZACIÓN 2026**", identificado con código **EBC-USNT-PL-00001, Versión N.° 2.1**, correspondiente a la Gestión 2026, que en calidad de **Anexo Único** forma parte integrante e indivisible de la presente Resolución Administrativa. El PISI aprobado constituye el instrumento institucional para establecer las directrices, responsabilidades, controles, mecanismos de gestión de riesgos, protección de activos de información, gestión de incidentes, continuidad y demás medidas destinadas a preservar la seguridad de la información de la EBC.

ARTÍCULO SEGUNDO.- DESIGNAR al servidor público **FÉLIX CHAMBI CONDE**, quien desempeña el cargo de **Técnico II en Sistemas y Nuevas Tecnologías**, dependiente del Área de Sistemas y Nuevas Tecnologías, como **RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN – RSI TITULAR DE LA EBC**, en concordancia con el Memorándum **MEM/GG/SMS/2026-00013, de fecha 14 de julio de 2026**. El RSI ejercerá sus funciones conforme a los Lineamientos PISI, el PISI aprobado mediante la presente Resolución Administrativa, la normativa vigente y las instrucciones emitidas por la Máxima Autoridad Ejecutiva.

ARTÍCULO TERCERO.- FUNCIONES DEL RSI.- El Responsable de Seguridad de la Información – RSI tendrá, entre otras, las siguientes funciones:

a) Coordinar y coadyuvar en la implementación del Plan Institucional de Seguridad de la Información – PISI.

b) Coordinar la gestión de riesgos de seguridad de la información.

c) Promover y realizar el seguimiento de la implementación de controles de seguridad de la información.

d) Coordinar la actualización del inventario, clasificación y valoración de los activos de información institucional.

e) Coordinar la gestión y reporte de incidentes de seguridad de la información conforme a la normativa y procedimientos establecidos por AGETIC y el CGII.

UNIDAD JURIDICA V°B° C.R.A.M. EBC

UNIDAD JURIDICA V°B° B.A.S.R.D.C. EBC

f) Coordinar la elaboración, actualización y seguimiento de procedimientos, instructivos y demás instrumentos derivados del PISI.
g) Realizar el seguimiento de los indicadores y métricas de seguridad de la información.
h) Promover actividades de capacitación y concientización dirigidas a las servidoras y servidores públicos de la EBC.
i) Coordinar con el Comité de Seguridad de la Información – CSI las acciones necesarias para la implementación, seguimiento, evaluación y mejora continua del PISI.
j) Coordinar con AGETIC y demás instancias competentes los asuntos relacionados con seguridad de la información.
k) Cumplir las demás funciones establecidas en los Lineamientos PISI, el PISI institucional y la normativa vigente.

ARTÍCULO CUARTO.- CONFORMAR el COMITÉ DE SEGURIDAD DE LA INFORMACIÓN – CSI DE LA EBC, de acuerdo con el tamaño de la estructura organizativa, volumen y complejidad de las operaciones institucionales, integrado por los siguientes miembros:

DESIGNACION DEL COMITÉ DE SEGURIDAD DE LA INFORMACION (CSI)		
COMITÉ DE SEGURIDAD	**NOMBRES Y APELLIDOS**	**CARGO DEL FUNCIONARIO**
Presidente del CSI	Ing. Sergio Mustafá Sáenz	Gerente General
Miembro del CSI	Lic. María Aleja Peñaranda Tapia	Gerente Administrativo Financiero
Miembro del CSI	Ing. Wilson Campero Laruta	Jefe Unidad de Planificación y Gestión de Calidad.
Miembro del CSI	Dra. Cecilia Aparicio Molina	Responsable de la Unidad Jurídica
Miembro del CSI	Ing. Felix Chambi Conde	Responsable del Área de Sistemas y Nuevas tecnologías.

ARTÍCULO QUINTO.- (PRESIDENCIA Y ORGANIZACIÓN DEL CSI). El Comité de Seguridad de la Información – CSI será presidido por el Gerente General de la EBC, en su condición de Máxima Autoridad Ejecutiva, quien podrá delegar sus funciones de presidencia conforme a la normativa aplicable.
El CSI establecerá su organización interna, forma de funcionamiento, periodicidad de reuniones, mecanismos de convocatoria, quórum y demás aspectos operativos mediante el instrumento que corresponda.

ARTÍCULO SEXTO.- (FUNCIONES DEL CSI). El Comité de Seguridad de la Información – CSI tendrá las siguientes funciones mínimas:
a) Revisar el Plan Institucional de Seguridad de la Información – PISI.
b) Promover la aprobación del PISI ante la Máxima Autoridad Ejecutiva.

c) Revisar los manuales, procedimientos e instructivos de seguridad de la información derivados del PISI.
d) Proponer estrategias para la implementación y fortalecimiento de controles de seguridad de la información.
e) Realizar seguimiento y control de los indicadores y métricas establecidos en el PISI.
f) Promover acciones de capacitación y concientización en seguridad de la información.
g) Analizar los riesgos institucionales relevantes en materia de seguridad de la información y proponer medidas de tratamiento.
h) Realizar seguimiento al cumplimiento del cronograma de implementación y regularización del PISI.
i) Promover la mejora continua de la seguridad de la información.
j) Conocer los informes periódicos presentados por el RSI sobre el estado de la seguridad de la información institucional.
k) Recomendar a la Máxima Autoridad Ejecutiva las acciones correctivas y preventivas necesarias.
l) Cumplir las demás funciones previstas en los Lineamientos PISI, el PISI institucional y la normativa vigente.

ARTÍCULO SÉPTIMO.- DISPONER que todas las Gerencias, Jefaturas, Unidades Organizacionales, servidoras y servidores públicos de la EBC, así como terceros que se encuentren comprendidos dentro del ámbito de aplicación del PISI, den estricto cumplimiento a las políticas, controles, responsabilidades, procedimientos y medidas de seguridad establecidos en el Plan Institucional de Seguridad de la Información aprobado mediante la presente Resolución Administrativa.

ARTÍCULO OCTAVO.- DISPONER la implementación, actualización y mantenimiento permanente del inventario y clasificación de los activos de información institucional, conforme a lo establecido en el PISI y sus anexos.

La clasificación de la información deberá efectuarse de conformidad con la Constitución Política del Estado, las disposiciones sobre transparencia y acceso a la información pública, protección de datos, confidencialidad, archivo y demás normativa aplicable, no pudiendo el inventario institucional constituirse por sí mismo en fundamento autónomo para declarar información reservada o confidencial fuera de los supuestos legalmente establecidos.

UNIDAD JURÍDICA VoBo C.R.A.M. EBC

UNIDAD JURÍDICA VoBo R.A.S.V.D.C. EBC

ARTÍCULO NOVENO.- DISPONER que el **RSI**, en coordinación con el **CSI** y las unidades organizacionales responsables de los activos de información, efectúe la identificación, valoración, evaluación y tratamiento de los riesgos de seguridad de la información, así como la implementación, seguimiento y documentación de los controles correspondientes, de acuerdo con la metodología establecida en el PISI.

ARTÍCULO DÉCIMO.- APROBAR la ejecución del cronograma de regularización y actualización correspondiente a la Gestión 2026 incorporado en el PISI, debiendo las unidades organizacionales responsables adoptar las acciones necesarias para el cumplimiento de las actividades y plazos establecidos.

El cronograma institucional no podrá interpretarse como ampliación, modificación o suspensión de los plazos establecidos por AGETIC, OFEP u otras autoridades competentes.

ARTÍCULO DÉCIMO PRIMERO.- INSTRUIR al Responsable de Seguridad de la Información – RSI y al Área de Sistemas y Nuevas Tecnologías, en coordinación con las unidades correspondientes, realizar las acciones necesarias para la presentación y/o registro del PISI aprobado ante AGETIC y la remisión de la documentación correspondiente a OFEP, conforme a los mecanismos, requisitos y procedimientos establecidos por las instancias competentes.

ARTÍCULO DÉCIMO SEGUNDO.- DISPONER que el RSI, en coordinación con las unidades correspondientes, cumpla con las obligaciones de reporte y atención de incidentes de seguridad de la información establecidas en el artículo 17 del Decreto Supremo N.° 2514, modificado por el Decreto Supremo N.° 5519, y conforme a los procedimientos establecidos por el Centro de Gestión de Incidentes Informáticos – CGII.

ARTÍCULO DÉCIMO TERCERO.- DEJAR SIN EFECTO, a partir de la entrada en vigencia de la presente Resolución Administrativa, la **Resolución Administrativa EBC N.° 0157/2023, de 26 de octubre de 2023**, únicamente en cuanto a la aprobación del Plan Institucional de Seguridad de la Información – PISI correspondiente a la versión anterior, quedando sustituido dicho instrumento por el **PISI – Actualización 2026, Versión N.° 2.1**, aprobado mediante la presente Resolución.

ARTÍCULO DÉCIMO CUARTO.- RESPONSABILIDAD DE LAS UNIDADES ORGANIZACIONALES Las Gerencias, Jefaturas y demás unidades organizacionales de la EBC serán responsables, en el ámbito de sus competencias, de implementar y cumplir las medidas de seguridad de la información previstas en el PISI, así como de proporcionar al RSI la información y documentación necesaria para el seguimiento, evaluación y mejora continua de los controles implementados.

ARTÍCULO DÉCIMO QUINTO.- DISPONER que la Unidad de Auditoria Interna, dentro del marco de sus competencias y de acuerdo con su planificación, considere la verificación del cumplimiento e implementación del PISI, así como de las medidas y controles de seguridad de la información que correspondan.

ARTÍCULO DÉCIMO SEXTO.- SEGUIMIENTO Y ACTUALIZACIÓN El RSI, en coordinación con el CSI, deberá realizar el seguimiento periódico de la implementación del PISI y promover su revisión y actualización cuando existan modificaciones normativas, tecnológicas, organizacionales, cambios relevantes en los riesgos institucionales o cuando las circunstancias así lo requieran.

ARTÍCULO DÉCIMO SÉPTIMO.- VIGENCIA.- La presente Resolución Administrativa entrará en vigencia a partir de la fecha de su suscripción, debiendo el PISI aprobado ser de cumplimiento obligatorio para todas las unidades y servidores públicos comprendidos en su ámbito de aplicación.

ARTÍCULO DÉCIMO OCTAVO.- CUSTODIA Y DIFUSIÓN El Área de Sistemas y Nuevas Tecnologías, en coordinación con el RSI y las unidades competentes, deberá disponer la custodia, control de versiones, difusión y accesibilidad institucional del PISI aprobado, garantizando que se mantenga disponible la versión vigente y se evite la utilización de documentos obsoletos.

ARTÍCULO DÉCIMO NOVENO.- NOTIFICACIÓN Y CUMPLIMIENTO.- Quedan encargadas del cumplimiento de la presente Resolución Administrativa la Gerencia General, el Área de Sistemas y Nuevas Tecnologías, el Responsable de Seguridad de la Información – RSI, el Comité de Seguridad de la Información – CSI y todas las unidades organizacionales de la EBC, en el marco de sus respectivas competencias.

ARTÍCULO VIGÉSIMO.- REGISTRO Y ARCHIVO.- La Unidad correspondiente procederá al registro, notificación, publicación interna y archivo de la presente

UNIDAD JURÍDICA VºBº R.A.M. EBC

Resolución Administrativa, debiendo incorporarse al expediente administrativo todos los antecedentes técnicos y legales que sustentan su emisión.

Regístrese, comuníquese, cúmplase y archívese.

Sergio Mustafa Saenz
GERENTE GENERAL
EMPRESA ESTRATÉGICA BOLIVIANA DE CONSTRUCCIÓN Y CONSERVACIÓN DE INFRAESTRUCTURA CIVIL-EBC

www.ebc.gob.bo
Av. Brasil N° 1636 Zona Miraflores, La Paz-Bolivia
Email: ebcbolivia@ebc.gob.bo
Telf.: (591-2)-2188100

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN - (PISI)

INSTANCIAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

ELABORADO POR:

Nombre:	Felix Chambi Conde
Cargo:	Técnico II en Sistemas y Nuevas Tecnologías
Fecha:	
Firma:	Felix Chambi Conde TÉCNICO II EN SISTEMAS Y NUEVAS TECNOLOGÍAS EMPRESA ESTRATÉGICA BOLIVIANA DE CONSTRUCCIÓN Y CONSERVACIÓN DE INFRAESTRUCTURA CIVIL-EBC

REVISADO Y APROBADO POR:

Nombre:	Ing. Sergio Mustafa Saenz
Cargo:	Gerente General - EBC
Fecha:	
Firma:	Sergio Mustafa Saenz GERENTE GENERAL EMPRESA ESTRATÉGICA BOLIVIANA DE CONSTRUCCIÓN Y CONSERVACIÓN DE INFRAESTRUCTURA CIVIL-EBC

Prohibida cualquier reproducción parcial o total de este documento sin autorización de la EBC

Contenido

1. INTRODUCCIÓN....3
2. MARCO INSTITUCIONAL....3
3. MARCO NORMATIVO....4
4. OBJETIVO....5
5. ALCANCE....5
6. ROLES Y RESPONSABILIDADES....5
6.1. Máxima Autoridad Ejecutiva (MAE)....5
6.2. Responsable de Seguridad de la Información (RSI)....6
6.3. Comité de Seguridad de la Información (CSI)....6
6.4. Gerencias, Jefaturas y Responsables....7
6.5. Servidoras y Servidores Públicos....7
6.6. Auditoría Interna....7
7. METODOLOGÍA DE GESTIÓN DE RIESGOS....7
7.1. Identificación, clasificación y valoración de activos de información....8
7.2. Evaluación del Riesgo....8
7.3. Tratamiento del Riesgo....9
7.4. Controles Implementados y por Implementar....10
7.5. Activos de información, evaluación, tratamiento del riesgo y controles establecidos....10
8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN....10
9. CONTROLES MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN....11
10. INDICADORES Y MÉTRICAS....12
11. CRONOGRAMA....12
12. ANEXOS....13
13. CONTROL DE CAMBIOS....13

UNIDAD DE SISTEMAS V°B° F.C.C. EBC

1. INTRODUCCIÓN

La Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil, consciente de la importancia de la seguridad de la información en su misión de ejecutar proyectos de construcción y conservación de infraestructura civil en todo el territorio nacional, presenta el Plan Institucional de Seguridad de la Información en el marco del Decreto Supremo N° 2514.

El Decreto Supremo N° 2514 y los lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público, establecen los estándares y protocolos que deben seguirse para asegurar la gestión adecuada de la seguridad de la información en las instituciones. Este marco legal es la base para el presente Plan.

El presente plan establece, salvaguardar la integridad, confidencialidad y disponibilidad de la información de la Empresa. En donde las instituciones/empresas están ahora interconectadas y en constante evolución tecnológica, la protección de nuestros datos y sistemas no es solo una obligación, sino también muestran la transparencia de nuestras operaciones.

Las políticas y normativas establecidas en el presente documento ayudarán a prevenir, detectar y responder ante incidentes de seguridad que puedan amenazar nuestra información. Además, de establecer roles y responsabilidades para todos los involucrados en la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil.

2. MARCO INSTITUCIONAL

Mediante Decreto Supremo No. 1020 de fecha 26 de octubre de 2011, se crea la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil, cuya sigla es "EBC", como una Empresa Pública Nacional Estratégica, con personería jurídica de derecho público, de duración indefinida y patrimonio propio, con autonomía de gestión administrativa, financiera, legal y técnica, que se encuentra bajo tuición del Ministerio de Obras Públicas, Servicios y Vivienda, misma que tiene por objeto la ejecución de proyectos de infraestructura civil en todo el territorio del Estado Plurinacional de Bolivia.

Las actividades y funciones principales de la Empresa Estratégica Bolivia de Construcción y Conservación de Infraestructura Civil - EBC, se divide en tres grandes grupos de servicios (Obra vendida, Laboratorio y Emulsiones Asfálticas), los cuales se relacionan entre si y forman parte de la cadena productiva de construcción.

Misión

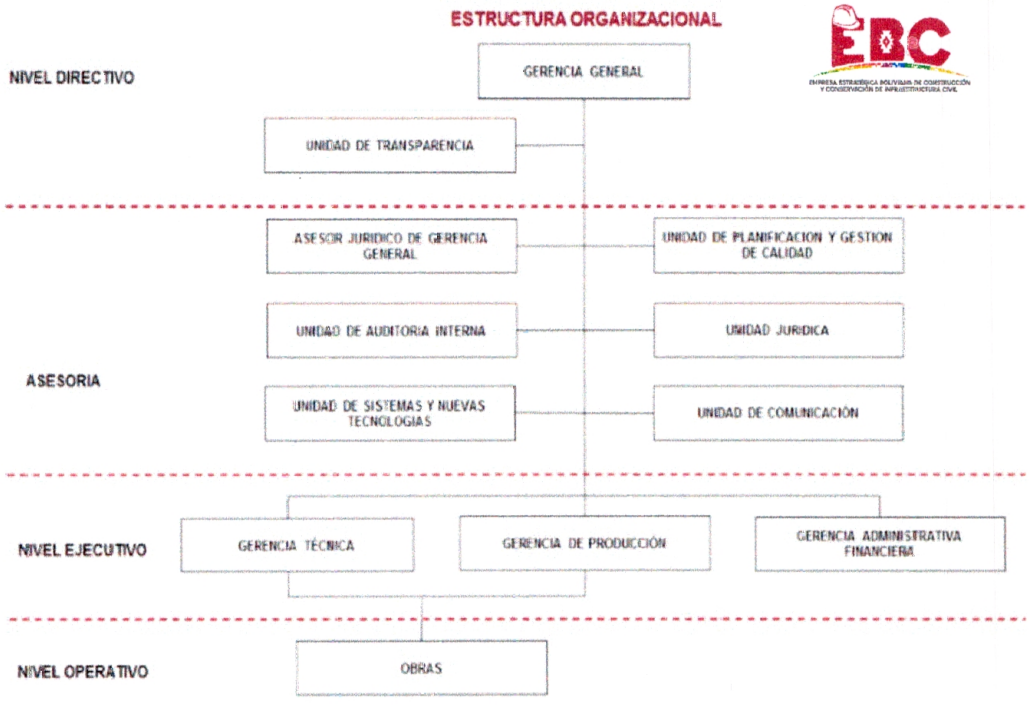
"Ejecutar proyectos de construcción de infraestructura civil en todo el territorio nacional, con eficiencia, eficacia, transparencia y calidad, para generar dividendos al Estado".

Visión

"Ser líder del mercado nacional de construcción, con especialización en pavimentación de carreteras, reconocidos por su alta calidad en la ejecución de obras, modelo de responsabilidad social y ambiental, con sostenibilidad técnica y financiera".

UNIDAD DE SISTEMAS V°B° EBC

ESTRUCTURA ORGANIZATIVA



Fuentes principales de Insumo

Para la elaboración del presente plan se identificó la siguiente documentación interna institucional:

a) Plan Estratégico Empresarial de la EBC (PEE). b) Plan Operativo Anual (POA). c) Documentación Administrativa.

- Reglamento Específico del sistema de organización administrativa de la EBC.
- Manual de organización y funciones del personal permanente de la EBC.
- Reglamento específico del sistema de administración de personal de la EBC.
- Reglamento específico del sistema de administración de bienes y servicios (RE-SABS).
- Manual de Funciones

3. MARCO NORMATIVO

- CPE - Constitución Política del Estado
- Decreto Supremo No. 29694 del 03 de septiembre de 2008 que establece la creación de Depósitos Aduaneros Bolivianos.
- Ley 164 - Ley General de telecomunicaciones, tecnologías de información y comunicación.
- Decreto Supremo No. 1793 Reglamento a la Ley 164.

UNIDAD DE SISTEMAS V°B° F.CH.C. EBC

- Decreto Supremo No. 3251 Aprueba Plan de Implementación de Gobierno Electrónico, Aprueba el Plan de Implementación de Software Libre y Estándares Abiertos.
- Decreto Supremo No. 2514 Creación Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación.
- Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público (AGETIC).
- Comunicado OFEP/DGE/SER N° 015/2026 de 29 de junio de 2026, Nota Externa AGETIC/NE/1466/2026 e Informe Técnico AGETIC-CGII/IT/0067/2026, referidos a la actualización e implementación de los Planes Institucionales de Seguridad de la Información (PISI).

4. OBJETIVO

Definir e implementar políticas, normativa, lineamientos, procedimientos y controles de seguridad de la información en la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC), 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 coma 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.

5. ALCANCE

Las políticas, normativas y procedimientos establecidos en el Plan de Seguridad de la Información (PISI), serán de cumplimiento obligatorio en todas las Unidades Organizacionales de la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil "EBC", empresas contratistas y terceros que interactúen con la empresa. Este plan tiene como objetivo principal establecer las directrices y acciones específicas que aseguren un nivel adecuado de protección para los activos de información y los recursos informáticos de la empresa.

6. ROLES Y RESPONSABILIDADES

6.1. Máxima Autoridad Ejecutiva (MAE)

La Máxima Autoridad Ejecutiva deberá:

- Estar informada sobre el estado de seguridad de la información de la entidad o institución pública bajo su tutela.
- 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 a la Ley 164).
- Designar al responsable de Seguridad de la Información (RSI).
- Asegurar que los objetivos y alcances del Plan Institucional de Seguridad de la Información sean compatibles con los objetivos del Plan Estratégico Institucional.
- En lo posible, destinar los recursos administrativos, económicos y humanos para la elaboración e implementación del Plan Institucional de Seguridad de la Información.

UNIDAD DE SISTEMAS V°B° F.O.C. EBC

- Aprobar el Plan Institucional de Seguridad de la Información de su entidad o institución.
- Cumplir y hacer cumplir el Plan Institucional de Seguridad de la Información de su entidad o institución.
- Asumir otras acciones a favor de la seguridad de la información.

6.2. Responsable de Seguridad de la Información (RSI)

(RSI), El responsable de Seguridad de la información, con perfil y experiencia en gestión de seguridad de la información, es designado por la MAE con memorándum MEM/GG/SMS/2026-00013 en fecha 14 de julio de 2026, y tiene como función principal la elaboración e implementación del PISI, y como funciones específicas, las siguientes:

- Gestionar, elaborar e implementar el Plan Institucional de Seguridad de la Información (PISI).
- Realizar la evaluación de riesgos de seguridad de la información en coordinación con los responsables de activos de información.
- Proponer la Política de Seguridad de la Información (PSI), que estará incorporada dentro del PISI.
- Gestionar el cumplimiento del PISI.
- 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.
- Sugerir prácticas de desarrollo de software seguro para generar procesos formales que tengan presentes los controles de seguridad necesarios para la entidad o institución.
- Coordinar la inducción, capacitación y comunicación del personal, en el marco del PISI.
- Gestionar y coordinar la atención y respuesta a incidentes de seguridad de la información en su entidad o institución.
- Coadyuvar en la gestión de contingencias tecnológicas.
- Proponer estrategias y acciones en mejora de la seguridad de la información.
- Promover la realización de auditorías al Plan Institucional de Seguridad de la Información.
- Gestionar la mejora continua de la seguridad de la información.
- Sugerir medidas de protección ante posibles ataques informáticos que puedan poner en riesgo las operaciones normales de la Institución.
- Realizar acciones de informática forense, en caso de ser necesario, para identificar, preservar, analizar y validar datos que puedan ser relevantes.
- Monitorear la implementación y uso de mecanismos de seguridad, que coadyuven a la reducción de los riesgos identificados.
- Otras funciones que resulten necesarias para preservar la seguridad de la información.

6.3. Comité de Seguridad de la Información (CSI)

La Máxima Autoridad Ejecutiva designará mediante resolución administrativa al personal que conformará el Comité de Seguridad de la Información (CSI), para gestionar, promover e impulsar iniciativas en seguridad de la información.

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).

UNIDAD DE SISTEMAS V°B° F.C.H.C. EBC

En caso de la existencia de Comités similares, se considerará la posibilidad de que estos asuman las funciones del CSI.

El CSI establecerá su organización interna y deberá desarrollar como mínimo las siguientes funciones:

- Revisar el Plan Institucional de Seguridad de la Información (PISI).
- Promover la aprobación del PISI a través de la MAE.
- 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.
- Proponer estrategias necesarias para la implementación y/o fortalecimiento de controles de seguridad en el marco de la mejora continua.
- Realizar el seguimiento y control de los indicadores y métricas establecidos y definir las acciones que correspondan al respecto.
- Promover la concientización y capacitación en seguridad de la información al interior de la entidad o institución pública.
- 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.
- Otras funciones que resulten necesarias para la seguridad de la información.

6.4. Gerencias, Jefaturas y Responsables

Tienen la obligación de promover el cumplimiento de las Política Institucional y Procedimientos de Seguridad de información.

6.5. 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).

6.6. 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.

7. METODOLOGÍA DE GESTIÓN DE RIESGOS

La Metodología de Gestión de Riesgos de la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil - EBC se ha desarrollado siguiendo los lineamientos del Plan Institucional de Seguridad de la Información (PISI) y las directrices del Consejo para las Tecnologías de Información y Comunicación (CTIC). La metodología se estructura en los siguientes pasos:

- Identificación, clasificación y valoración de activos de la Información
- Evaluación del riesgo
- Tratamiento del riesgo
- Controles implementados y por implementar

UNIDAD DE SISTEMAS V°B° F.C.H.C. EBC

7.1. Identificación, clasificación y valoración de activos de información

De acuerdo a los lineamientos para la elaboración del PISI, la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil "EBC", ha realizado la identificación de activos de información a través del relevamiento y recopilación de información con los responsables de la administración de las mismas, la misma que requiere de protección frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta vital para la empresa es la que se denomina activo de información.

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

- Información - Datos que materializan la información.
- Claves criptográficas - codificación.
- Servicios - que se necesitan para poder organizar el sistema.
- Aplicaciones informáticas (Software) - que permiten manejar los datos
- Equipamiento informático (Hardware) - que permiten hospedar datos, aplicaciones y servicios.
- Redes de comunicaciones - que permiten intercambiar datos
- Soportes de información - dispositivos de almacenamiento de datos.
- Equipamiento auxiliar - que complementa el material informático.
- Instalaciones - ambientes utilizados.
- Personal - que explotan u operan todos los elementos anteriormente citados.

Para el inventario de activos de información y la clasificación de la misma, se tomó en cuenta los lineamientos del CTIC, considerando los siguientes aspectos:

- Activo de información identificado.
- Descripción del activo de información.
- Clasificación del activo en base al tipo definido.
- Ubicación física del activo, es decir donde se encuentra.
- Unidad Organizacional responsable de gestionar el activo de información identificado.
- Custodio, encargado de la custodia o resguardar del 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 realizado, es un resumen de los activos con los que cuenta la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil "EBC".

7.2. Evaluación del Riesgo

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

De forma posterior al inventario, 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.

ESCALA DE VALORACIÓN DEL RIESGO DE LA INFORMACIÓN

UNIDAD DE SISTEMAS V°B° F.C.C.C. EBC

Escala de Valoración	Nivel
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, 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?

7.3. Tratamiento del Riesgo

Con el fin de buscar la toma de decisiones, se realiza el análisis de los riesgos identificados, y se proponen controles, basándose en los controles mínimos requeridos y establecidos en los lineamientos adoptados como metodología, 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 PISI, 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 a 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 par completo el riesgo, mediante el retiro de una actividad, condiciones o conjunto de actividades ya sean planificadas a 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 solo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

UNIDAD DE SISTEMAS V°B° F.Q.M.C. EBC

7.4. Controles Implementados y por Implementar

Los controles implementados y por implementar producto del PISI, 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.

7.5. Activos de información, evaluación, tratamiento del riesgo y controles establecidos

De lo expuesto y en base a la metodología de gestión de riesgos de la EBC, Anexo adjunto, se estructura, la identificación y valoración de activos de información, seguida de una evaluación exhaustiva del riesgo. Posteriormente, se aplican acciones específicas para tratar el riesgo, considerando opciones como la aceptación, reducción, retención, evitación o transferencia. Los controles implementados y por implementar se definen cuidadosamente, proporcionando una estructura para la seguridad de la información en la EBC.

8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Dentro del Plan Institucional de Seguridad de la Información (PISI) se establecen los siguientes lineamientos generales:

- Reconocemos que la información constituye un activo esencial para la prestación eficiente de nuestros servicios y para tomar decisiones fundamentadas. Por esta razón, existe un compromiso a proteger nuestras propiedades más valiosas como parte integral de nuestra estrategia orientada a la continuidad del negocio, la gestión de riesgos y la promoción de una cultura de seguridad.
- En sintonía con las necesidades actuales, la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil "EBC", implementa un modelo de gestión de seguridad de la información que permite identificar y minimizar los riesgos asociados con nuestros datos, sino que también contribuye a la reducción de costos operativos y financieros. Este enfoque establece una cultura de seguridad y asegura el cumplimiento de los requisitos legales pertinentes.
- Todos los servidores públicos, personal externo, proveedores y cualquier persona con responsabilidades relacionadas con las fuentes, repositorios y recursos de procesamiento de información de la empresa deben seguir los lineamientos detallados en este documento y en otros documentos pertinentes. Estos lineamientos son fundamentales para mantener la confidencialidad, la integridad y la disponibilidad de nuestra información.
- La Política de Seguridad de la Información de nuestra empresa se basa en políticas, normas y procedimientos específicos que orientan el manejo adecuado de nuestra información. Cabe destacar que el Comité de Seguridad de la Información tiene la autoridad para modificar esta política según las necesidades de revisión periódica o cuando sea necesario ajustarla a nuevas circunstancias o regulaciones aplicables.

UNIDAD DE SISTEMAS V°B° F.C.H.C. EBC

En ese entendido se ha elaborado la versión 2 de La Política de Seguridad de la Información, de la Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil "EBC".

9. CONTROLES MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN

- **Seguridad en Recursos Humanos:** Se implementarán procedimientos de selección y capacitación para el personal, buscando una comprensión de las políticas de seguridad de la información de la EBC. Se definirán medidas para la gestión adecuada de las responsabilidades de seguridad de los empleados durante su permanencia y al finalizar su relación laboral con la empresa.
- **Gestión de Activos de Información:** Identificaremos, clasificaremos y protegeremos los activos de información más relevantes para la EBC. Se definirán procedimientos para el manejo seguro de los activos durante todo su ciclo de vida, desde la adquisición hasta la disposición, garantizando su integridad y confidencialidad.
- **Control de Accesos:** Se Implementarán controles de acceso adecuados, autorizaciones basadas en roles. Los accesos a los sistemas y datos estarán limitados a personas autorizadas, se llevará registros de las actividades de acceso.
- **Criptografía:** Se definirán y utilizaremos técnicas de cifrado para proteger la información confidencial durante el almacenamiento y la transmisión, asegurando la integridad y confidencialidad de los datos.
- **Seguridad Física y Ambiental:** Implementaremos medidas de seguridad física para proteger los activos de información contra amenazas físicas, así como controles ambientales para prevenir daños por condiciones climáticas o ambientales adversas.
- **Seguridad de las Operaciones:** Estableceremos procedimientos operativos seguros para garantizar la continuidad del negocio y reducir al mínimo el riesgo de interrupciones. Esto incluirá la gestión segura de cambios, la supervisión proactiva de los sistemas y la protección contra software malicioso.
- **Seguridad de las Comunicaciones:** Aseguraremos la confidencialidad e integridad de las comunicaciones electrónicas mediante el uso de tecnologías seguras de transmisión de datos, protegiendo la información durante su transferencia a través de redes internas y externas.
- **Desarrollo, Mantenimiento y Adquisición de Sistemas:** Integraremos medidas de seguridad en todas las etapas del ciclo de vida del desarrollo del software y adquisición de sistemas. Esto incluirá la evaluación y gestión de riesgos, así como pruebas de seguridad regulares.
- **Gestión de Incidentes de Seguridad de la Información:** Estableceremos un proceso para la notificación, gestión y resolución de incidentes de seguridad de la información. Se asignarán responsabilidades y se documentarán los incidentes para análisis posterior y para prevenir futuros incidentes similares.
- **Plan de Contingencias Tecnológicas:** Desarrollaremos un plan de contingencia tecnológica que incluirá procedimientos para la respuesta a desastres y la recuperación de datos. Se realizarán pruebas periódicas para asegurar la efectividad del plan.
- **Cumplimiento:** Se realizarán auditorías coordinadas, de manera periódica para evaluar el cumplimiento de estas políticas y controles de seguridad de la información. Se implementarán medidas correctivas en caso de no cumplimiento.

Estos controles mínimos de seguridad de la información se implementarán para garantizar la protección, confidencialidad e integridad de los datos de la EBC.

UNIDAD DE SISTEMAS V°B° F.O.C. EBC

10. INDICADORES Y MÉTRICAS

En nuestro Plan de Seguridad de la Información, la evaluación de criticidades y la efectividad de los controles implementados en nuestros activos prioritarios se basarán en indicadores y métricas específicas. Cada Unidad Organizacional de la EBC enfrenta sus propios riesgos, por lo tanto, se requiere métricas personalizadas vinculadas a los objetivos de seguridad y los procesos específicos necesarios. Los indicadores aplicados durante la valoración inicial, que medirán la reducción de la criticidad en los activos prioritarios, se integran en:

- **Identificación de Activos de Información:** Definición y documentación exhaustiva de los activos de información.
- **Análisis de Riesgos:** Evaluación detallada utilizando una metodología de riesgos para identificar riesgos y amenazas en cada activo de información.
- **Nivel de Seguridad Existente:** Evaluación del nivel de seguridad en sistemas, servicios, aplicaciones e infraestructura, incluyendo incidentes y actualizaciones.
- **Definición de Planes de Acción:** Desarrollo de planes de acción a corto, mediano y largo plazo, detallados en el Cronograma de Implementación.
- **Implementación de Mecanismos de Seguridad:** Aplicación de controles específicos en las áreas establecidas en las Políticas de Seguridad de la Información.

Las métricas utilizadas serán medidas definidas y adaptadas a nivel estratégico (progreso del cronograma) y a nivel táctico y operativo (procesos y controles de la Política de Seguridad de la Información). En todos los niveles, las métricas se caracterizarán por ser:

- **Relevantes y Contextuales:** Se alinearán específicamente con los objetivos de seguridad y los contextos operativos de cada unidad organizacional.
- **Medibles y Cuantificables:** Permitirán una evaluación objetiva y cuantitativa del progreso y la efectividad de los controles implementados.
- **Adaptables y Evaluables:** Se ajustarán según sea necesario para reflejar cambios en las amenazas, tecnologías y procesos de la organización.

Estas métricas son específicas, medibles cualitativa y cuantitativamente, alcanzables, relevantes y repetibles en períodos de tiempo específicos. Utilizamos la métrica de eficacia o efectividad, que representa el porcentaje de disminución de los riesgos, indicando el grado en el que se cumplen nuestros objetivos de seguridad. Estos indicadores y métricas son fundamentales para evaluar nuestro progreso y asegurar una mejora continua en nuestra postura de seguridad de la información.

11. CRONOGRAMA

El cronograma de actividades y tareas para implementar el Plan de Seguridad de la Información (PISI) en nuestra empresa, está en función al relevamiento de los activos de información, los lineamientos sobre la composición y estructura del Plan y la Política de Seguridad de la Información para una empresa estratégica de las características de la EBC. A continuación, se presenta un cronograma de actividades para llevar a cabo la implementación del PISI inicial:

Cronograma de Regularización y Actualización del PISI (Gestión 2026)

UNIDAD DE SISTEMAS V°B° F.C.U. EBC

En cumplimiento del Comunicado OFEP/DGE/SER N° 015/2026 de 29 de junio de 2026, se establece el siguiente cronograma de regularización, con un plazo máximo de 45 días calendario desde la publicación del comunicado en el sistema SER:

Hito	Eje Estratégico	Descripción de Actividades	Fecha Estimada de Cierre	Responsable
1	Resguardo y protección del patrimonio informacional	Reunión de coordinación técnica con AGETIC para validar la estructura y alcance del PISI	20/07/2026	Felix Chambi Conde
2	Resguardo y protección del patrimonio informacional	Actualización del inventario y clasificación de la información institucional (Anexo VI)	27/07/2026	Felix Chambi Conde
3	Seguridad y continuidad de la información física y digital	Elaboración y/o actualización del documento PISI conforme a lineamientos vigentes de AGETIC	03/08/2026	Felix Chambi Conde
4	Estructura y Gestión integral de la información	Revisión y aprobación interna del PISI por la Máxima Autoridad Ejecutiva (MAE)	10/08/2026	Máxima Autoridad Ejecutiva (MAE)
5	Transparencia y control de la información	Presentación formal del PISI ante la AGETIC y remisión de copia a la OFEP	13/08/2026	Felix Chambi Conde

12. ANEXOS

Anexo I: Matriz de Activos de información - Valoración de Activos

Anexo II: Activos de Información - Análisis del Riesgo Activos.

Anexo III: Matriz de Valoración de Riesgos.

Anexo IV: Controles Implementados y por Implementar

Anexo V: Matriz de Reporte por Eje Estratégico (Actualización 2026)

Anexo VI: Inventario y Clasificación de Información Institucional (Actualización 2026)

13. CONTROL DE CAMBIOS

Versión	Fecha	Cambio Efectuado
1	12/10/2018	Edición inicial
2	26/10/2023	Actualización del documento inicial, incorporando mejores prácticas y políticas que se alinean adecuadamente a las necesidades y objetivos de nuestra empresa.
2.1	13/08/2026	Actualización en cumplimiento del Comunicado OFEP/DGE/SER N° 015/2026, incorporación de la Matriz de Reporte por Eje Estratégico, del Inventario y Clasificación de Información Institucional.

UNIDAD DE SISTEMAS V°B° F.C.C. EBC

ANEXOS

UNIDAD DE SISTEMAS V°B° F.C.H.C. EBC

ANEXO I

MATRIZ DE ACTIVOS DE INFORMACIÓN - VALORACIÓN DE ACTIVOS

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

INVENTARIO DE ACTIVOS IDENTIFICADOS							VALORACION DE ACTIVOS				GESTION	
N.	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad	Valoración Final	Fecha de Ingreso	Fecha Salida
1	Servidor Lenovo SR530 (Storage D1212)	Servidor PROXMOX de aplicaciones y bases de datos	Hardware	Centro de Procesamiento de Datos - CPD	Sistemas y Nuevas Tecnologías	Sistemas y Nuevas Tecnologías	MUY ALTO	ALTO	ALTO	**ALTO**	1/6/2022	
2	CPD	Centro de Procesamiento de Datos	Equipamiento Informático	Oficina Central	Sistemas y Nuevas Tecnologías	Sistemas y Nuevas Tecnologías	MUY ALTO	ALTO	ALTO	**ALTO**	1/6/2022	
3	SIAS	Sistema de Almacenes y Suministros	Software - Aplicaciones Informáticas	CPD - Servidores	Sistemas y Nuevas Tecnologías	Sistemas y Nuevas Tecnologías	ALTO	ALTO	ALTO	**ALTO**	1/2/2015	
4	SIACO	Sistema de Correspondencia	Software - Aplicaciones Informáticas	CPD - Servidores	Unidad de Sistemas y Nuevas Tecnologías	Unidad de Sistemas y Nuevas Tecnologías	BAJO	MEDIO	MEDIO	**MEDIO**	11/8/2014	1/7/2022
5	SIPV	Sistema de Pasajes y Viáticos	Software - Aplicaciones Informáticas	CPD - Servidores	Unidad de Sistemas y Nuevas Tecnologías	Unidad de Sistemas y Nuevas Tecnologías	BAJO	BAJO	BAJO	**MEDIO**	1/3/2016	1/7/2022
6	ZIMBRA	Correo Electrónico Institucional	Software - Aplicaciones Informáticas	CPD - Servidores	Unidad de Sistemas y Nuevas Tecnologías	Unidad de Sistemas y Nuevas Tecnologías	ALTO	ALTO	MEDIO	**ALTO**	1/8/2023	

UNIDAD DE SISTEMAS V°B° F.C.C. EBC

ANEXO I

MATRIZ DE ACTIVOS DE INFORMACIÓN - VALORACIÓN DE ACTIVOS

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

INVENTARIO DE ACTIVOS IDENTIFICADOS							VALORACION DE ACTIVOS				GESTION	
N.	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad	Valoración Final	Fecha de Ingreso	Fecha Salida
7	SGM	Sistema Integrado que gestiona los módulos (Correspondencia, Pasajes y Viáticos, Boletas de permiso del personal)	Software - Aplicaciones Informáticas	CPD - Servidores	Unidad de Sistemas y Nuevas Tecnologías	Unidad de Sistemas y Nuevas Tecnologías	MUY ALTO	ALTO	MEDIO	**ALTO**	1/8/2022	
8	Equipos Informáticos	Computadoras, impresoras y escáner	Equipamiento Informático	Unidades Organizacionales de la EBC	Activos Fijos	Usuarios	ALTO	ALTO	MEDIO	**ALTO**	10/1/2015	
9	Documentación Física	Contratos, planillas de seguimiento, control y pago de obras, actas de ingreso y salida de material	Datos o Información	Unidades Organizacionales de la EBC	Unidades Organizacionales de la EBC	Usuarios	MEDIO	ALTO	ALTO	**ALTO**	1/1/2012	
10	Documentos Contables	Certificaciones Presupuestarias, comprobantes de pago	Datos o Información	Contabilidad	Contabilidad	Contabilidad	ALTO	ALTO	MEDIO	**ALTO**	1/1/2012	
11	Archivo Físico	Ambientes de Archivo Central que almacenan la documentación física de la EBC	Datos o Información	Ambientes de archivo	Responsable de Archivo	Responsable de Archivo	ALTO	MUY ALTO	ALTO	**ALTO**	1/12/2013	
12	UPS	Sistema de Alimentación Ininterrumpida	Equipamiento Auxiliar	CPD - Oficina Central	Sistemas y Nuevas Tecnologías	Sistemas y Nuevas Tecnologías	ALTO	ALTO	BAJO	**MEDIO**	1/1/2018	

UNIDAD DE SISTEMAS V°B° F.CH.C. EBC

ANEXO I

MATRIZ DE ACTIVOS DE INFORMACIÓN - VALORACIÓN DE ACTIVOS

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

INVENTARIO DE ACTIVOS IDENTIFICADOS							VALORACION DE ACTIVOS				GESTION	
N.	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad	Valoración Final	Fecha de Ingreso	Fecha Salida
13	Backups archivos digitales de gestiones pasadas	Archivos digitales de exfuncionarios	Información	Servidor de Backup	Unidad de Sistemas y Nuevas Tecnologías	Unidad de Sistemas y Nuevas Tecnologías	MEDIO	MUY ALTO	ALTO	**MEDIO**	1/1/2015	
14	Internet	Internet Entel FIBRA	Redes de Comunicaciones	CPD - Oficina Central	Unidad de Sistemas y Nuevas Tecnologías	Unidad de Sistemas y Nuevas Tecnologías	ALTO	ALTO	MEDIO	**ALTO**	11/5/2013	
15	Página WEB	Página WEB Institucional	Servicios	CPD - Oficina Central	Unidad de Sistemas y Nuevas Tecnologías	Unidad de Sistemas y Nuevas Tecnologías	ALTO	ALTO	MEDIO	**ALTO**	1/5/2023	
16	Antivirus	Antivirus Institucional	Software - Aplicaciones Informáticas	Servidores y Computadoras	Unidad de Sistemas y Nuevas Tecnologías	Unidad de Sistemas y Nuevas Tecnologías	ALTO	ALTO	MEDIO	**ALTO**	1/6/2023	

UNIDAD DE SISTEMAS V°B° F.C.E. EBC

ANEXO II

ACTIVOS DE INFORMACIÓN - ANÁLISIS DEL RIESGO ACTIVOS

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

INVENTARIO DE ACTIVOS IDENTIFICADOS				ANALISIS DE RIESGO			VALORACION DE RIESGO		
N.	Activo	Descripción	Tipo	Amenazas	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel Riesg
1	Servidor Lenovo SR530 (Storage D1212)	Servidor PROXMOX de aplicaciones y bases de datos	Hardware	Acceso no autorizado, Fallos de hardware, Ataque Cibernético, malware	El servidor Proxmox hospeda máquinas virtuales con aplicaciones críticas y bases de datos.	Configuraciones incorrectas, contraseñas débiles, falta de mantenimiento.	PROBABLE	CRITICO	ALTO
2	CPD	Centro de Procesamiento de Datos (Instalación física que aloja los servidores de la EBC)	Equipamiento Informático	Cortes de energía, ambientes, incendios, inundaciones.	Su ubicación y tamaño impiden la implementación de normativa mínima e indispensable	Falta de sistemas de detección de fuego, piso falso, falta de respaldo eléctrico.	POCO PROBABLE	CRITICO	ALTO
3	SIAS	Sistema de Almacenes y Suministros	Software - Aplicaciones Informáticas	Ataques cibernéticos, malware, errores de programación.	La aplicación es accesible a través de la red interna y/o externa.	Versión y plataforma obsoleta, débiles controles en validación de datos.	POCO PROBABLE	MODERADO	BAJO
4	SIACO	Sistema de Correspondencia	Software - Aplicaciones Informáticas	Robo de información	El sistema está habilitado para solo consultas.	Extracción de información	POCO PROBABLE	MENOR	BAJO
5	SIPV	Sistema de Pasajes y Viáticos	Software - Aplicaciones Informáticas						
6	ZIMBRA	Correo Electrónico Institucional	Software - Aplicaciones Informáticas	Fuga de información, Phishing, malware adjunto.	Correo electrónico bajo software libre	Falta de conciencia de seguridad por parte de los usuarios.	PROBABLE	MODERADO	MEDI
7	SGM	Sistema de integrado que gestiona el módulo (Correspondencia, Pasajes y Viáticos, Boletas de permiso del personal)	Software - Aplicaciones Informáticas	Acceso No autorizado	Los usuarios en su mayoría no cambian las contraseñas facilitadas por Sistemas en su ingreso al sistema, o periódicamente no realizan los cambios de contraseñas	La falta de mecanismos de identificación y autenticación de usuarios, como ser (Login, Password, Tokens, Aplicaciones.)	MUY PROBABLE	SEVERO	ALTO
8	Equipos Informáticos	Computadoras, Impresoras y escáner	Equipamiento Informático	Robo, malware, mal uso.	Equipos distribuidos en toda la empresa.	Falta de políticas de seguridad física, uso inadecuado, manipulación por el personal.	POCO PROBABLE	MODERADO	BAJO

UNIDAD DE SISTEMAS V°B° F.C.C. EBC

ANEXO II

ACTIVOS DE INFORMACIÓN - ANÁLISIS DEL RIESGO ACTIVOS

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

INVENTARIO DE ACTIVOS IDENTIFICADOS				ANALISIS DE RIESGO			VALORACION DE RIESGO		
N.	**Activo**	**Descripción**	**Tipo**	**Amenazas**	**Situación**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
9	Documentación Física	Contratos, planillas de seguimiento, control y pago de obras, actas de ingreso y salida de material	Datos o Información	Robo, pérdida accidental, daños por agua/incendio, acceso no autorizado.	Documentos almacenados en archivadores en las oficinas.	Almacenamiento inadecuado (expuestos). Falta cultura de archivo.	POCO PROBABLE	MODERADO	**BAJO**
10	Documentos Contables	Certificaciones Presupuestarias, comprobantes de pago	Datos o Información	Robo de Documentos	Personas externas roban documentos físicos	Descuido del personal del área	POCO PROBABLE	SEVERO	**MEDIO**
11	Archivo Físico	Ambientes de Archivo Central que almacenan la documentación física de la EBC	Datos o Información	Robo, pérdida accidental, deterioro, daños, acceso no autorizado.	El área de Archivo se encuentra en una ubicación accesible y no adecuada.	Área de almacenamiento inadecuado, Riesgos de daños de los documentos.	PROBABLE	SEVERO	**ALTO**
12	UPS	Sistema de Alimentación Ininterrumpida	Equipamiento Auxiliar	Cortes de energía, sobrecargas, fallos del sistema UPS.	UPS que proporcionan energía de respaldo a los equipos críticos.	Falta de mantenimiento, capacidad insuficiente	PROBABLE	SEVERO	**ALTO**
13	Backups archivos digitales de gestiones pasadas	Archivos digitales de exfuncionarios	Información	Acceso no autorizado, malware, pérdida de datos, fallos del sistema, robo de datos.	Datos almacenados en discos físicos, computadora de archivos, sistemas de almacenamiento.	Pérdida de datos sensibles, fallo del disco, violación de privacidad	POCO PROBABLE	SEVERO	**MEDIO**
14	Internet	Internet Entel FIBRA	Redes de Comunicaciones	Ataques de Intercepción (datos en tránsito y acceder a información confidencial). Los usuarios pueden descargar archivos maliciosos o hacer clic en enlaces engañosos.	La conexión a Internet es una actividad recurrente e importante de información y comunicación.	Configuraciones de red inseguras, falta de cifrado.	MUY PROBABLE	SEVERO	**ALTO**
15	Página WEB	Página WEB	Servicios	Ataques cibernéticos,	Importantes para la	Código de la aplicación	POCO	MENOR	**BAJO**

UNIDAD DE SISTEMAS V°B° F.C.H.C. EBC

ANEXO II

ACTIVOS DE INFORMACIÓN - ANÁLISIS DEL RIESGO ACTIVOS

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

INVENTARIO DE ACTIVOS IDENTIFICADOS				ANALISIS DE RIESGO			VALORACION DE RIESGO		
N.	Activo	Descripción	Tipo	Amenazas	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
				(Phishing-crear sitios web falsos). Inyección de Código malicioso.	presencia en línea de la Empresa.	débil. Contraseñas débiles	PROBABLE		
16	Antivirus	Antivirus Institucional	Software - Aplicaciones Informáticas	Virus, troyanos y ransomware comprometen los sistemas. Ataques de día cero (antes de que se publiquen los parches).	El software antivirus es esencial para proteger sistemas contra malware y otras amenazas. Detecta, previene y elimina software malicioso.	Sin actualizaciones, el antivirus no puede detectar nuevas amenazas. Configuraciones inapropiadas pueden dejar brechas en la protección.	PROBABLE	CRITICO	**ALTO**

UNIDAD DE SISTEMAS Vº Bº F.C.H.C. EBC

ANEXO III

MATRIZ DE VALORACIÓN DE RIESGOS

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

PROBABILIDADA					
Cierta/inminente	Bajo	Medio	Alto	Critico	Critico
Muy probable	Bajo	Medio	Alto	7, 14	Critico
Probable	Irrelevante	Bajo	6	11, 12	1, 16
Poco Probable	Irrelevante	4, 15	3, 8, 9	10, 13	2
Improbable	Irrelevante	Irrelevante	Irrelevante	Bajo	Bajo
	Irrelevante	**Menor**	**Moderado**	**Severo**	**Critico**

IMPACTO

UNIDAD DE SISTEMAS V°B° F.A.C.

ANEXO IV

CONTROLES IMPLEMENTADOS Y POR IMPLEMENTAR

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

N.	Activo	Tipo	Dispo.	Inte.	Confi.	Control	Actividad	Existe	Incluir	Justificación Inclusión	Justificación Exclusión
1	Servidor Lenovo SR530 (Storage D1212)	Hardware	MUY ALTO	ALTO	ALTO	Control de accesos y monitoreo	Realizar un cronograma de mantenimiento y actualización de los Servidores. Realizar análisis de rendimiento anual.	No	Si	Continuidad y rendimiento adecuados de las aplicaciones y bases de datos asegurar la operación de los sistemas.	
2	CPD	Equipamiento Informático	MUY ALTO	ALTO	ALTO	Gestión Ambiental, infraestructura	Implementar en la medida de lo posible con sistema mínimos de seguridad y continuidad operativa de un CPD (Sensores de fuego, piso falso, aire acondicionado, cable estructurado, sistema de energía ininterrumpida)	No	No		Los Ambientes de la Oficina Central no reúnen y no cuentan con las condiciones mínimas necesarias para implementar un CPD bajo normas internacionales, se analizará la posibilidad de nuevas instalaciones.
6	ZIMBRA	Software - Aplicaciones Informáticas	ALTO	ALTO	MEDIO	Capacitación y formación	Realizar capacitaciones de concientización sobre seguridad de correo electrónico.	No	Si	Reducir la probabilidad de que los usuarios caigan en ataques de phishing y comprometan la seguridad.	
7	SGM	Software - Aplicaciones Informáticas	MUY ALTO	ALTO	MEDIO	Control de Accesos	Elaborar procedimientos de Administración de usuarios, para el control de altas, bajas y modificación de los derechos de acceso.	No	Si	Establecer y normar el acceso a los sistemas, reducir la probabilidad de robos de identidad, por descuidos o contraseñas muy débiles o fáciles.	
8	Equipos Informáticos	Equipamiento Informático	ALTO	ALTO	MEDIO	Normativa y Procedimientos	Elaborar procedimientos de mantenimiento preventivo y correctivo del parque informático de la empresa. Así como también realizar inventarios periódicos de equipos.	No	Si	Velar por un funcionamiento adecuado de los equipos. Llevar un control actualizado de los equipos.	
9	Documentación Física	Datos o Información	MEDIO	ALTO	ALTO	Control de accesos	Implementar políticas de acceso restringido y almacenar documentos sensibles	No	No		Los ambientes actuales no reúnen las condiciones adecuadas para

UNIDAD DE SISTEMAS V°B° F.C.H.C. EBC

ANEXO IV

CONTROLES IMPLEMENTADOS Y POR IMPLEMENTAR

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

N.	Activo	Tipo	Dispo.	Inte.	Confi.	Control	Actividad	Existe	Incluir	Justificación Inclusión	Justificación Exclusión
							clasificados en Archivo.				implementar áreas de almacenamiento restringido ni de ambientes protegidos, se analizara la posibilidad de nuevas instalaciones.
10	Documentos Contables	Datos o Información	ALTO	ALTO	MEDIO	Control de accesos	Mantener y controlar el acceso (chapa digital - acceso restringido)	Si	Si	Se reduce la probabilidad de pérdida por robos o daños, con la restricción del acceso al área Contable.	
11	Archivo Físico	Datos o Información	ALTO	MUY ALTO	ALTO	Seguridad física y ambiental, seguridad física en áreas e instalaciones	Implementar políticas de acceso restringido y almacenar documentos sensibles clasificados en Archivo.	No	No		Los ambientes actuales no reúnen las condiciones adecuadas para implementar áreas de almacenamiento restringido ni de ambientes protegidos, se analizara la posibilidad de nuevas instalaciones.
12	UPS	Equipamiento Auxiliar	ALTA	ALTA	BAJO	Seguridad física ambiental - CPD	Adquirir e implementar una UPS de mayor capacidad, monitorizar la carga y autonomía de la UPS.	Si	Si	Garantizar que la UPS tenga la capacidad adecuada y funcione correctamente durante cortes de energía para mantener la continuidad del servicio	
13	Backups archivos digitales de gestiones pasadas	Información	MEDIO	MUY ALTO	ALTO	Control de Accesos	Adquisición de un servidor de archivos, con seguridad y protección de datos (RAID)	No	Si	Asegurar que los datos estén protegidos contra accesos no autorizados y pérdida, y garantizar la disponibilidad y confidencialidad de la información almacenada.	
14	Internet	Redes de Comunicaciones	ALTO	ALTO	MEDIO	Gestión de Red	Cumplir con los pagos periódicos de los servicios de internet para garantizar la operación y accesibilidad a los	Si	Si	Los sistemas informáticos básicos y esenciales son accedidos por Internet, los proyectos y obras	

UNIDAD DE SISTEMAS Vº Bº F.C.M.G. EBC

ANEXO IV

CONTROLES IMPLEMENTADOS Y POR IMPLEMENTAR

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

N.	Activo	Tipo	Dispo.	Inte.	Confi.	Control	Actividad	Existe	Incluir	Justificación Inclusión	Justificación Exclusión
							Sistemas de la Empresa.			principalmente realizan sus operaciones por este medio.	
15	Antivirus	Software - Aplicaciones Informáticas	ALTO	ALTO	MEDIO	Seguridad de las Comunicaciones	Renovación anual de licencias del Antivirus para mantener las firmas y el motor del antivirus actualizado.	Si	Si	Es importante la actualización anual del Antivirus, para minimizar la probabilidad de infección en las plataformas tecnológicas de la EBC.	

Dispo.: Disponibilidad

Inte.: Integridad

Confi.: Confidencialidad

ANEXO V

MATRIZ DE REPORTE POR EJE ESTRATÉGICO

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

N°	Eje Estratégico	Estado de Implementación	Evidencia/Documentación	Observaciones
1	Alta disponibilidad de la información física y digital	[√] Implementado	Respaldos (backups) periódicos de información crítica	Mecanismos vigentes, sujetos a revisión periódica
2	Resguardo y protección del patrimonio informacional físico y digital	[√] Implementado	Inventario y clasificación de la información institucional (Anexo VI); políticas de retención, conservación y disposición final; controles de acceso físico y lógico.	Categorías de información en proceso de actualización, conforme al Anexo VI adjunto
3	Seguridad y continuidad de la información física y digital	[√] Implementado	Documento PISI en actualización conforme a cronograma (Anexo VIII); aplicación del Lineamiento de Seguridad SEG-001-1; procedimientos de gestión de incidentes de seguridad.	PISI en proceso de actualización formal ante la AGETIC, conforme al cronograma adjunto
4	Transparencia y control de la información física y digital	[√] Implementado	Registros de auditoría y trazabilidad de accesos y modificaciones.	Implementado sobre los sistemas críticos de la entidad
5	Infraestructura y gestión integral de la información física y digital	[√] Implementado	Designación formal de responsable de la gestión de la información (Anexo VII).	Responsable designado conforme al Anexo VII adjunto

UNIDAD DE SISTEMAS V°B° F.C.H.C. EBC

ANEXO VI

INVENTARIO Y CLASIFICACIÓN DE INFORMACIÓN INSTITUCIONAL

Institución Pública: Empresa Estratégica Boliviana de Construcción y Conservación de Infraestructura Civil (EBC)

Categoría de Información	Implementado	En proceso	No iniciado	Observaciones
Documentos institucionales y normativos	[√]			
Información financiera		[√]		
Documentos administrativos	[√]			
Información de control interno	[√]			
Documentación legal y tributaria		[√]		
Recursos humanos		[√]		
Para empresas productivas - industriales (si corresponde)			[√]	No aplica al rubro de la empresa
Comercialización			[√]	No aplica al rubro de la empresa
Inversiones			[√]	No aplica al rubro de la empresa

UNIDAD DE SISTEMAS V°B° F.C.C. EBC