EMPRESA ESTATAL DE TELEVISIÓN

"BOLIVIA TV"

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

Tipo	Código	Versión
Plan	P-BTV-RSI-01	02

Aprobado mediante Resolución Administrativa N°043/2023
de 31 de octubre de 2023

RESOLUCIÓN ADMINISTRATIVA N° 043/2023

La Paz, 31 de octubre de 2023

VISTOS Y CONSIDERANDOS:

Que el artículo 103 de la **Constitución Política del Estado** determina que: *"I. El Estado garantizará el desarrollo de la ciencia y la investigación científica, técnica y tecnológica en beneficio del interés general. Se destinarán los recursos necesarios y se creará el sistema estatal de ciencia y tecnología. II. El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación. III. El Estado, las universidades, las empresas productivas y de servicio públicas y privadas, y las naciones y pueblos indígena originario campesinos, desarrollarán y coordinarán procesos de investigación, innovación, promoción, divulgación, aplicación y transferencia de ciencia y tecnología para fortalecer la base productiva e impulsar el desarrollo integral de la sociedad, de acuerdo con la ley".*

Que el numeral 3 del parágrafo II del artículo 299 de la norma constitucional prevé que: *"II. Las siguientes competencias se ejercerán de forma concurrente por el nivel central del Estado y las entidades territoriales autónomas: (...) 3. Ciencia, tecnología e investigación."*

Que la **Ley Nº 164 de 08 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación**, señala que: *"La presente Ley tiene por objeto establecer el régimen general de telecomunicaciones y tecnologías de información y comunicación, del servicio postal y el sistema de regulación, en procura del vivir bien garantizando el derecho humano individual y colectivo a la comunicación, con respeto a la pluralidad económica, social, jurídica, política y cultural de la totalidad de las bolivianas y los bolivianos, las naciones y pueblos indígena originario campesinos, y las comunidades interculturales y afrobolivianas del Estado Plurinacional de Bolivia"*

Que el artículo 72 de la antedicha Ley refiere que: *"I. 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."*

Que el artículo 4 del **Decreto Supremo Nº 0078 de 15 de abril de 2009**, estipula que BOLIVIA TV, tiene por objeto la prestación del servicio de televisión a través de la emisión y reproducción de sus señales en todo el territorio boliviano, constituyéndose en un medio de comunicación, educación e información que contribuya a la promoción de los valores éticos, morales y cívicos de las diferentes culturas, fortaleciendo la integración del Estado Plurinacional de Bolivia.

Que el inciso h) del artículo 11 del precitado Decreto Supremo, faculta al Gerente General aprobar mediante Resolución Administrativa los actos que le competen.

Que el **Decreto Supremo Nº 1793 de 13 de noviembre de 2013**, que reglamenta la Ley Nº 164 de 08 de agosto de 2011, dispone en su parágrafo VI del artículo 3 que: *"(...) VI. Respecto a la seguridad informática. a) Seguridad informática: Es el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionado con ésta y, especialmente, la información contenida o circulante; b) Seguridad de la información: La seguridad de la información es 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; c) Plan de contingencia: Es un instrumento que comprende métodos y el conjunto de 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".*

Que el inciso d) del parágrafo II del artículo 4 del antedicho Decreto Supremo, indica que: *"(...) Tratamiento de datos personales: Los servicios de certificación digital en cuanto al tratamiento de datos personales, se regirán por los siguientes principios: (...) d) Seguridad: Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la i información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento;"*

Que mediante **Decreto Supremo Nº 2514 de 09 de septiembre de 2015**, se crea la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC y los Comités Interinstitucionales de

Simplificación de Trámites. Asimismo, los incisos f) e i) del artículo 7 del precitado Decreto Supremo, establece que la AGETIC tiene las siguientes funciones: *"(...) f) Establecer los lineamientos técnicos en seguridad de información para las entidades del sector público;(...) i) Elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática".*

Que el parágrafo I y los incisos b) y c) del parágrafo II del artículo 8 del precitado Decreto Supremo, indica que: *"I. Se crea el Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC. II. El CGII tiene las siguientes funciones: (...) b) Establecer los lineamientos para la elaboración de Planes Institucionales de Seguridad de la Información de las entidades del sector público; c) Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público;(...)".*

Que el parágrafo III del artículo 17 del Decreto Supremo Nº 2514 descrito precedentemente, menciona entre las obligaciones de seguridad informática que: *"(...) Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII."*

Que el **Decreto Supremo N° 3251 del 12 de julio de 2017**, aprueba el Plan de Implementación de Gobierno Electrónico, que establece como una de las líneas estratégicas la seguridad informática y de la información.

Que mediante **Resolución Ministerial Nº 028/23 de 31 de enero de 2023**, emitido por el Ministerio de la Presidencia, se designó al ciudadano JULIO FERNANDO VALDIVIA RODRÍGUEZ como Gerente General de la Empresa Estatal de Televisión "BOLIVIA TV".

Que mediante **Resolución Administrativa Nº 093/2018 de 17 de septiembre de 2018**, el Gerente General de Bolivia TV, designó al Comité de Seguridad de la Información de la Empresa Estatal de Televisión Bolivia TV, conformado por las siguientes autoridades: Gerente General (Presidente); Gerente Administrativo Financiero; Gerente de Marketing y Ventas; Gerente Técnico; Director de Deportes y Creatividad; y al Jefe Nacional de Noticias.

Que el inciso g), numeral 6.1.1 del punto 6 de los **Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público**, elaborado por los miembros del Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB) y el Centro de Gestión de Incidentes Informáticos (CGII), señalan que entre las responsabilidades de la Máxima Autoridad Ejecutiva, respecto a la seguridad de la información, está el de Aprobar el Plan Institucional de Seguridad de la Información de su entidad o institución.

Que por Informe Técnico CITE: BTV/RSI/INF N° 001/2023 de fecha 31 de octubre de 2023, los Responsables de Seguridad de la Información, vía el Comité de Seguridad de la Información de la Empresa Estatal de Televisión "BOLIVIA TV", informan que, el "Plan Institucional de Seguridad de la Información" en su primera versión fue aprobado en la gestión 2018, cuya Metodología de Análisis y Gestión de Riesgos fue "Daft"; y de acuerdo al cronograma debía implementarse en la gestión 2019, sin embargo, a consecuencia de la alta rotación del personal, no se llegó a concretar dicho plan, además del cambio de gobierno y la aparición de pandemia COVID-19, en consecuencia y bajo los lineamientos de la AGTETIC, se actualizó el "Plan Institucional de Seguridad de la Información" de acuerdo a la Metodología de Análisis y Gestión de Riesgos "Magerit". Asimismo, del análisis del documento, las metodologías que se utilizan para la elaboración de un PISI fueron la ISO 27001, como una norma internacional emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una empresa. Por otra parte señala, dejar sin efecto el Plan de Seguridad de la Información de la Empresa Estatal de Televisión "BOLIVIA TV" en su primera versión, aprobado mediante Resolución Administrativa N° 096/2018 de 19 de septiembre de 2018, quedando obsoleto e inaplicable.

Que el precitado informe **concluye** que: *"(...) se procedió a la actualización del **Plan de Seguridad de la Información** de la Empresa Estatal de Televisión "BOLIVIA TV" en su segunda versión, en coordinación con miembros del Comité de Seguridad de la Información, documento que se adecua a los lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público (SEG – 001: elaborado por los miembros del consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia y el Centro de Gestión de Incidentes Informáticos) y la estructura establecida en el Reglamento de Documentos Normativos Internos"*; y **recomienda**, remitir a la Dirección Jurídica Nacional el aludido informe y el plan de Seguridad de la Información, para la elaboración del Informe Legal y la aprobación mediante Resolución Administrativa.

DIRECCIÓN JURÍDICA NACIONAL V°B° José Pedro Ogarte Iriarte "BOLIVIA TV"

DIRECCIÓN JURÍDICA V°B° Abg. Hanz E. Lanchipa Ch. "BOLIVIA TV"

Que a través de Informe Legal BTV/DJN Nº 433/2023 de 31 de octubre de 2023, emitido por la Dirección Jurídica Nacional **concluye** lo siguiente: *"**1.** La solicitud de aprobación del Plan Institucional de Seguridad de la Información de la Empresa Estatal de Televisión Bolivia TV, en su segunda versión, propuesto por los Responsables de Seguridad de la Información, vía el Comité de Seguridad de la Información de la Empresa Estatal de Televisión "BOLIVIA TV", no contraviene normativa en actual vigencia, puesto que el mismo se encuentra bajo los lineamentos técnicos en seguridad de información para las entidades del sector público, establecidos por la AGETIC y respaldado mediante por el Informe Técnico CITE: BTV/RSI/INF N° 001/2023 de fecha 31 de octubre de 2023; y **2.** El Plan Institucional de Seguridad de la Información en su primera versión, aprobado mediante Resolución Administrativa Nº 096/2018 de 19 de septiembre de 2018, al no haber sido concretado a consecuencia de la alta rotación del personal, el cambio de gobierno en la gestión 2019 y la aparición de pandemia COVID-19 en la gestión 2020, corresponde dejar sin efecto, a través de la correspondiente Resolución Administrativa"*; y, **recomienda**, la suscripción de una Resolución Administrativa que apruebe el "Plan Institucional de Seguridad de la Información de la Empresa Estatal de Televisión Bolivia TV", en su segunda versión, en aplicación del inciso h) del artículo 11 del Decreto Supremo 078 de 15 de abril de 2009 y el inciso g), numeral 6.1.1 del punto 6 de los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público.

POR TANTO:

El Gerente General de la Empresa Estatal de Televisión "BOLIVIA TV", en uso de sus facultades conferidas por Decreto Supremo Nº 0078 de 15 de abril de 2009, la Resolución Ministerial Nº 028/23 de 31 de enero de 2023, emitido por el Ministerio de la Presidencia y los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público.

RESUELVE:

ARTÍCULO PRIMERO.- APROBAR el **"PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN" DE LA EMPRESA ESTATAL DE TELEVISIÓN "BOLIVIA TV"**, en su segunda versión, que en anexo forma parte integrante de la presente Resolución Administrativa.

ARTÍCULO SEGUNDO.- El Comité de Seguridad de la Información de la Empresa Estatal de Televisión "Bolivia TV", queda encargado de la ejecución y cumplimiento de la presente Resolución Administrativa.

ARTÍCULO TERCERO.- DEJAR SIN EFECTO, la Resolución Administrativa Nº 096/2018 de 19 de septiembre de 2018, que aprueba Plan Institucional de Seguridad de la Información de la Empresa Estatal de Televisión "Bolivia TV", en su primera versión.

Regístrese, comuníquese, cúmplase y archívese.

DIRECCIÓN JURÍDICA NACIONAL V°B° José Pedro Ugarte Imaña "BOLIVIA TV"

Lic. Julio Fernando Valverde Rodriguez
GERENTE GENERAL
Empresa Estatal de Televisión
"BOLIVIA TV"

DIRECCIÓN JURÍDICA V°B° Abg. Hans E. Lanchipa Ch. "BOLIVIA TV"

EMPRESA ESTATAL DE TELEVISIÓN

"BOLIVIA TV"

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

Tipo	Código	Versión
Plan	P-BTV-RSI-01	02

Aprobado mediante Resolución Administrativa N°043/2023
de 31 de octubre de 2023

CONTROL DE EMISIÓN DEL DOCUMENTO

Nombre del documento: Plan Institucional de Seguridad de la Información.
Versión: 02.
Unidad promotora: Responsables de Seguridad de la Información - RSI.
Unidad revisora: Comité de Seguridad de la Información – CSI.

	Cargo	Firma	Sello
Actualizado por miembros RSI:	**Técnico en Sistemas**		Marco Antonio Huanca Layme TÉCNICO DE SISTEMAS Empresa Estatal de Televisión "BOLIVIA TV"
	Profesional en Proyectos		Richard Nina Calla PROFESIONAL EN PROYECTOS Empresa Estatal de Televisión "Boliva TV"
	Responsable de Legajos Técnicos		Ing. Leidy Sorca Calle Mamani RESPONSABLE DE LEGAJOS TÉCNICOS EMPRESA ESTATAL DE TELIVISIÓN BOLIVIA TV
	Técnico de Transmisión		Lic. Ricardo Favio Mamani Condori TÉCNICO DE TRANSMISIÓN EMPRESA ESTATAL DE TELEVISION BOLIVIA TV
	Técnico Laboratorio de Generación de Señal		Osbaldo I. Parrado Mamani TECNICO LABORATORIO DE GENERACIÓN DE SEÑAL EMPRESA ESTATAL DE TELEVISIÓN "BOLIVIA TV"
Revisado por miembros CSI:	**Gerente Administrativo Financiero a.i.**		MSc. Tatiana Terceros Cortéz GERENTE ADMINISTRATIVO FINANCIERO a.i. EMPRESA ESTATAL DE TELEVISIÓN "BOLIVIA TV"

	Gerente de Marketing y Ventas		GERENTE DE MARKETING Y VENTAS EMPRESA ESTATAL DE TELEVISIÓN "BOLIVIA TV"
	Gerente Técnico		Victor Wilmer Mamani Cáceres GERENTE TÉCNICO Empresa Estatal de Televisión "BOLIVIA TV"
	Gerente de Informaciones (Jefe Nacional de Noticias)		Yandira B. Claros Ale GERENTE DE INFORMACIONES Empresa Estatal de Televisión "BOLIVIA TV"
	Jefe de Deportes y Creatividad		Marco Antonio Llanos Calderon JEFE DE DEPORTES Y CREATIVIDAD BOLIVIA TV
Aprobado por:	**Gerente General**		Lic. Julio Fernando Valdivia Rodriguez GERENTE GENERAL Empresa Estatal de Televisión "BOLIVIA TV"

CONTROL DE CAMBIOS

N° Versión	Descripción del cambio	N° de Resolución	Fecha de aprobación
01	Primera versión del documento	RA 096/2018	19/09/2018
02	Actualización de la Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información - Magerit.	RA 043/2023	31/10/2023

INDICE

1. INTRODUCCIÓN 1

2. MARCO NORMATIVO 2

3. DIAGNÓSTICO INSTITUCIONAL 5

3.1. TÉRMINOS, DEFINICIONES Y SIGLAS 5

3.2. OBJETIVOS DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN 8

3.2.1. OBJETIVO GENERAL 8

3.2.2. OBJETIVOS ESPECÍFICOS 8

4. ALCANCE DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN 8

5. METODOLOGÍA DE GESTIÓN DE RIESGOS 10

5.1. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN 11

5.2. EVALUACIÓN DE RIESGO 29

5.3. MATRIZ DE VALORACIÓN DEL RIESGO 42

5.4. TRATAMIENTO DE RIESGO 42

5.5. CONTROLES MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN 59

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 59

6.1. OBJETIVO GENERAL 59

6.2. OBJETIVO ESPECIFICO 60

6.3. ROLES Y RESPONSABILIDADES 60

6.4. DESIGNACIÓN Y RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN 60

6.4.1. Funciones del RSI 60

6.5. DESIGNACIÓN Y FUNCIONES DEL COMITÉ DE LA SEGURIDAD DE LA INFORMACIÓN 61

6.7. INDICADORES Y METRICAS 62

6.8. CUMPLIMIENTO 63

7. DIFUSIÓN 63

8. SANCIONES 64

9. HISTORICO DE CAMBIOS 64

10. CRONOGRAMA DE IMPLEMENTACIÓN 64

INDICE

1. **INTRODUCCIÓN** 1
2. **MARCO NORMATIVO** 2
3. **DIAGNÓSTICO INSTITUCIONAL** 5
   - 3.1. TÉRMINOS, DEFINICIONES Y SIGLAS 5
   - 3.2. OBJETIVOS DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN 8
     - 3.2.1. OBJETIVO GENERAL 8
     - 3.2.2. OBJETIVOS ESPECÍFICOS 8
4. **ALCANCE DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN** 8
5. **METODOLOGÍA DE GESTIÓN DE RIESGOS** 10
   - 5.1. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN 11
   - 5.2. EVALUACIÓN DE RIESGO 29
   - 5.3. MATRIZ DE VALORACIÓN DEL RIESGO 42
   - 5.4. TRATAMIENTO DE RIESGO 42
   - 5.5. CONTROLES MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN 59
6. **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** 59
   - 6.1. OBJETIVO GENERAL 59
   - 6.2. OBJETIVO ESPECIFICO 60
   - 6.3. ROLES Y RESPONSABILIDADES 60
   - 6.4. DESIGNACIÓN Y RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN 60
     - 6.4.1. Funciones del RSI 60
   - 6.5. DESIGNACIÓN Y FUNCIONES DEL COMITÉ DE LA SEGURIDAD DE LA INFORMACIÓN 61
   - 6.7. INDICADORES Y METRICAS 62
   - 6.8. CUMPLIMIENTO 63
7. **DIFUSIÓN** 63
8. **SANCIONES** 64
9. **HISTORICO DE CAMBIOS** 64
10. **CRONOGRAMA DE IMPLEMENTACIÓN** 64

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

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

El presente Plan busca establecer los lineamientos generales en materia de seguridad de la información de Empresa Estatal de Televisión "BOLIVIA TV".

Mediante Decreto Supremo N° 078 de 15 de abril de 2009, crea la Empresa Estatal de Televisión denominada "BOLIVIA TV"; la cual determina su naturaleza jurídica, objeto y patrimonio; además de establecer la conformación y atribuciones de su Directorio y su Gerente General.

Se constituye como persona jurídica de derecho público, de duración indefinida, con patrimonio propio y autonomía de gestión administrativa, financiera, legal y técnica, bajo tuición del Ministerio de Presidencia.

BOLIVIA TV, tiene por objeto la prestación de servicio de televisión a través de la emisión y reproducción de sus señales en todo el territorio boliviano, constituyéndose en un medio de comunicación, educación e información, que contribuya a la promoción de los valores éticos, morales y cívicos de las diferentes culturas, fortaleciendo la integración del Estado Plurinacional de Bolivia.

Tanto la misión, la visión como los principios y valores forman parte de la cultura organizacional de BOLIVIA TV, gracias a que la dinámica y el clima laboral se orienta en principios y metas comunes; en este sentido, resulta fundamental comprender las diferencias. El objetivo de una declaración de Misión es describir el «qué» y «hacia quién» de una empresa, la declaración de Visión refiere al «porqué» y al «cómo».

En este entendido, se ha definido como la Misión Empresarial de BOLIVIA TV con el siguiente texto:

"Somos la principal empresa estratégica de comunicación audiovisual del Estado Plurinacional, que produce y difunde contenidos plurales para informar y educar, con valores éticos, morales y cívicos a las diversas culturas y nacionalidades de Bolivia"

El modelo de Plan Institucional de Seguridad de Información se encuentra alineado en el marco de referencia del documento de Seguridad SEG-001; "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público"

Es por ello es que se asume la responsabilidad de implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) que permita lograr niveles adecuados de

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

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

El presente Plan busca establecer los lineamientos generales en materia de seguridad de la información de Empresa Estatal de Televisión "BOLIVIA TV".

Mediante Decreto Supremo N° 078 de 15 de abril de 2009, crea la Empresa Estatal de Televisión denominada "BOLIVIA TV"; la cual determina su naturaleza jurídica, objeto y patrimonio; además de establecer la conformación y atribuciones de su Directorio y su Gerente General.

Se constituye como persona jurídica de derecho público, de duración indefinida, con patrimonio propio y autonomía de gestión administrativa, financiera, legal y técnica, bajo tuición del Ministerio de Presidencia.

BOLIVIA TV, tiene por objeto la prestación de servicio de televisión a través de la emisión y reproducción de sus señales en todo el territorio boliviano, constituyéndose en un medio de comunicación, educación e información, que contribuya a la promoción de los valores éticos, morales y cívicos de las diferentes culturas, fortaleciendo la integración del Estado Plurinacional de Bolivia.

Tanto la misión, la visión como los principios y valores forman parte de la cultura organizacional de BOLIVIA TV, gracias a que la dinámica y el clima laboral se orienta en principios y metas comunes; en este sentido, resulta fundamental comprender las diferencias. El objetivo de una declaración de Misión es describir el «qué» y «hacia quién» de una empresa, la declaración de Visión refiere al «porqué» y al «cómo».

En este entendido, se ha definido como la Misión Empresarial de BOLIVIA TV con el siguiente texto:

"Somos la principal empresa estratégica de comunicación audiovisual del Estado Plurinacional, que produce y difunde contenidos plurales para informar y educar, con valores éticos, morales y cívicos a las diversas culturas y nacionalidades de Bolivia"

El modelo de Plan Institucional de Seguridad de Información se encuentra alineado en el marco de referencia del documento de Seguridad SEG-001; "Lineamientos para la elaboración e implementación de los Planes Instituciones de Seguridad de la Información de las entidades del sector público"

Es por ello es que se asume la responsabilidad de implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) que permita lograr niveles adecuados de

seguridad para los activos de información institucional de BOLIVIA TV considerados relevantes, de tal manera garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

2. MARCO NORMATIVO

La elaboración del presente documento se enmarca en el mandato institucional respaldado por:
El inciso a) del Artículo 22 del Decreto Supremo No 29894, de 7 de febrero de 2009, de Organización del Órgano Ejecutivo, que establece que: "El Ministerio de la Presidencia es el Ente rector de Gobierno Electrónico y de Tecnologías de Información y Comunicación para el Sector público del Estado Plurinacional de Bolivia, siendo el encargado de establecer las políticas, lineamientos y normativa específica para su implementación, seguimiento y control".

El Artículo 2 del Decreto Supremo N° 2514, sobre la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC, como "una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica y patrimonio propio, bajo tuición del Ministerio de la Presidencia".

Lo señalado en los artículos 9, 10 y 11 del Decreto Supremo N° 2514 acerca de la creación del Consejo para las Tecnologías de Información y Comunicación para formular y presentar propuestas de políticas, normativa, programas y proyectos de Gobierno Electrónico y Tecnologías de Información y Comunicación por parte de las entidades del ámbito gubernamental normativo concerniente a la seguridad de la información incluye:

- El Parágrafo I del Artículo 72 de la Ley N° 164 de 8 de agosto 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 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 8 (Plan de contingencia) del Decreto Supremo N° 1793, de 13 de noviembre de 2013, que menciona 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"*.

- El Decreto Supremo N° 2514 de 9 de septiembre de 2015, en los siguientes artículos, incisos o disposiciones transitorias:
  - ❖ Inciso f) del Artículo 7, que sostiene 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"*.
  - ❖ Inciso i) del Artículo 7, que establece entre las funciones de la AGETIC, "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".
  - ❖ Parágrafo I del Artículo 8, de creación del "Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC".
  - ❖ Inciso c) del Parágrafo II del Artículo 8, que menciona como una de las funciones del Centro de Gestión de Incidentes Informáticos – CGII, "Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público".
  - ❖ Parágrafo III del Artículo 17, que 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 inciso f) del Artículo 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 8 (Plan de contingencia) del Decreto Supremo N° 1793, de 13 de noviembre de 2013, que menciona 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".

El Decreto Supremo N° 2514 de 9 de septiembre de 2015, en los siguientes artículos, incisos o disposiciones transitorias:

- Inciso f) del Artículo 7, que sostiene 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".
- Inciso i) del Artículo 7, que establece entre las funciones de la AGETIC, "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".
- Parágrafo I del Artículo 8, de creación del "Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC".
- Inciso c) del Parágrafo II del Artículo 8, que menciona como una de las funciones del Centro de Gestión de Incidentes Informáticos – CGII, "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 de aprobación del Plan de Implementación de Gobierno Electrónico, que establece como una de las líneas estratégicas la seguridad informática y de la información.

El Plan Estratégico Empresarial de la Empresa Estatal de Televisión "BOLIVIA TV" correspondiente al periodo 2021 – 2025, aprobado mediante Resolución de Directorio N°005/2022 de fecha 13 de julio de 2022, que establece la Acción 1.1.4.2: "Contar con una red televisiva que presta servicios y promociona en todos los niveles del estado la ideología y pensamiento propio de las diferentes identidades plurinacionales".

El Plan Operativo Anual, Anteproyecto de Presupuesto de la gestión 2024, aprobado mediante Resolución de Directorio N°002/2023 de 06 de septiembre de 2023, que establece el presupuesto a ejecutar por cada una de las actividades a desarrollar, para llegar al cumplimiento de las Acciones a Corto Plazo.

El Manual de Organización y Funciones aprobado mediante Resolución Administrativa N°018/2021 de 12 de marzo de 2021 y modificaciones aprobadas mediante Resolución Administrativa N°023/2021 de 31 de marzo de 2021, que tiene por objeto definir la estructura organizacional, los niveles jerárquicos, dependencia, relaciones de coordinación y los objetivos de cada unidad organizacional, así como la descripción de las funciones de las áreas y/o unidades organizacionales.

El "Plan Institucional de Seguridad de la Información" en su primera versión fue aprobado en la gestión 2018, mediante Resolución Administrativa N° 096/2018 de fecha 19 de septiembre de 2018. Sin embargo, a consecuencia de la alta rotación del personal, la declaración de Cuarentena Total en el territorio del Estado Plurinacional de Bolivia, contra el contagio y propagación del Coronavirus (COVID-19), estableciendo la suspensión de actividades públicas y privadas en atención a la declaración de emergencia sanitaria nacional. Por lo mencionado, se ha perdido el control de las implementaciones, además hubo el cambio de gobierno y rotación de personal designado como RSI y CSI.

3. DIAGNÓSTICO INSTITUCIONAL

La Empresa Estatal de Televisión "BOLIVIA TV", fue creada el 15 de abril de 2009, mediante Decreto Supremo N°078 "BOLIVIA TV", se constituye como persona jurídica de derecho público, de duración indefinida, con patrimonio propio y autonomía de gestión administrativa, financiera, legal y técnica, bajo tuición del Ministerio de la Presidencia.

La Empresa Estatal de Televisión "BOLIVIA TV", tiene por finalidad la prestación del servicio de televisión a través de la emisión y reproducción de sus señales en todo el territorio boliviano.

La Empresa Estatal de Televisión "BOLIVIA TV", realiza la generación, procesamiento y difusión de su señal a través de equipamiento de generación y transmisión, los cuales hacen uso del desarrollo de aplicaciones para la administración de la señal audiovisual, solo se tomó en cuenta la aplicación, más no la protección total de la información y tampoco su verificación de seguridad que se procesa diariamente; los mismos pueden llegar a ser afectados a la empresa a través de ataques de hackers, denegación de servicio DoS y entre otros.

Se realizaron esfuerzos importantes a fin de protegerse de ataques informáticos, provenientes de la red de internet conforme avanza la tecnología.

3.1. 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 empresa.

Responsable del activo de Información: Servidor público de nivel jerárquico que tiene las responsabilidades y atribuciones de establecer los requisitos de seguridad y la clasificación de la información relacionada al activo, según el alcance definido del proceso al cual pertenece la misma.

Custodio de activo de información: El servidor público encargado de administrar y hacer efectivo los controles de seguridad, que el responsable del activo de la información haya definido.

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

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

Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos.

Disponibilidad: Propiedad de ser accesible y utilizable por solicitud de una entidad autorizada.

Amenaza: Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en una organización.

Riesgo: Combinación de la probabilidad de un evento adverso y su consecuencia.

Vulnerabilidad: Debilidad de un activo o control, que puede ser explotada por una amenaza.

Impacto: Cambio adverso en la operación normal de un proceso de la institución pública.

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

Seguridad de la Información: La seguridad de la información se entiende como la preservación de las siguientes características:

- ✓ **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- ✓ **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- ✓ **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- ✓ **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- ✓ **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- ✓ **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- ✓ **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- ✓ **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- ✓ **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- ✓ **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- ✓ **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- ✓ **Tecnología de la Información:** Se refiere al hardware y software operados por el Organismo o por un tercero que procese la información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- ✓ **Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.
- ✓ **Administración de Riesgos:** Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- ✓ **Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
- ✓ **Responsable de Seguridad Informática:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.
- ✓ **Incidente de Seguridad**: Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de comp0utadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.
- ✓ **Tecnología de la Información:** Se refiere al hardware y software operados por la parte técnica o por un tercero que procese información, para llevar a cabo una función propia del equipo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Cuadro 1. ABREVIACIONES EMPLEADAS EN EL PISI.

SIGLA	DESCRIPCIÓN
ISO 27001:2015	Norma técnica del comité ISO (Sistema de Gestión de Seguridad de Información)
CSI	Comité de Seguridad de Información
RSI	Responsable de Seguridad de Información
BIA	Análisis de impacto al negocio
AGETIC	Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación
CTIC-EPB	Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional del Bolivia

CGI	Centro de Gestión de Incidentes Informáticos
PISI	Plan Institucional de Seguridad de la Información
MAE	Máxima Autoridad Ejecutiva
BOLIVIA TV	Empresa Estatal de Televisión – BOLIVIA TV

3.2. OBJETIVOS DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

3.2.1. OBJETIVO GENERAL

Establecer lineamientos que permitan proteger la información de BOLIVIA TV a través de acciones de Seguridad de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos de seguridad alineados en el contexto de direccionamiento estratégico 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 flujo de información audiovisual, mantenimiento y soporte de sistemas de información de la empresa.

3.2.2. OBJETIVOS ESPECÍFICOS

- ✓ Proteger los activos de información de BOLIVIA TV.
- ✓ Resguardar la información general de contenido e imagen de BOLIVIA TV.
- ✓ Identificar los riegos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- ✓ Optimizar las decisiones de seguridad de la información en apoyo a los objetivos institucionales.
- ✓ Monitorear los procesos de la información para verificar los resultados.
- ✓ Socializar en la institución en materia de la Seguridad de la Información, cuyo objetivo primordial será la preservación de la confidencialidad, integridad y disponibilidad de la información y recomendaciones de seguridad.
- ✓ Analizar el riesgo al cual están expuestos los activos de información, con la ayuda de la metodología MAGERIT y los responsables de la seguridad de información.
- ✓ Difundir en forma planificada entre todo el personal de la institución el objetivo de preservación de la información.
- ✓ Evitar la pérdida de imagen como organismo estratégico y coordinador de las políticas de fomento de desarrollo científico y tecnológico del país.
- ✓ Evitar la interrupción total o parcial del servicio de radiodifusión que presta el canal a la ciudadanía.

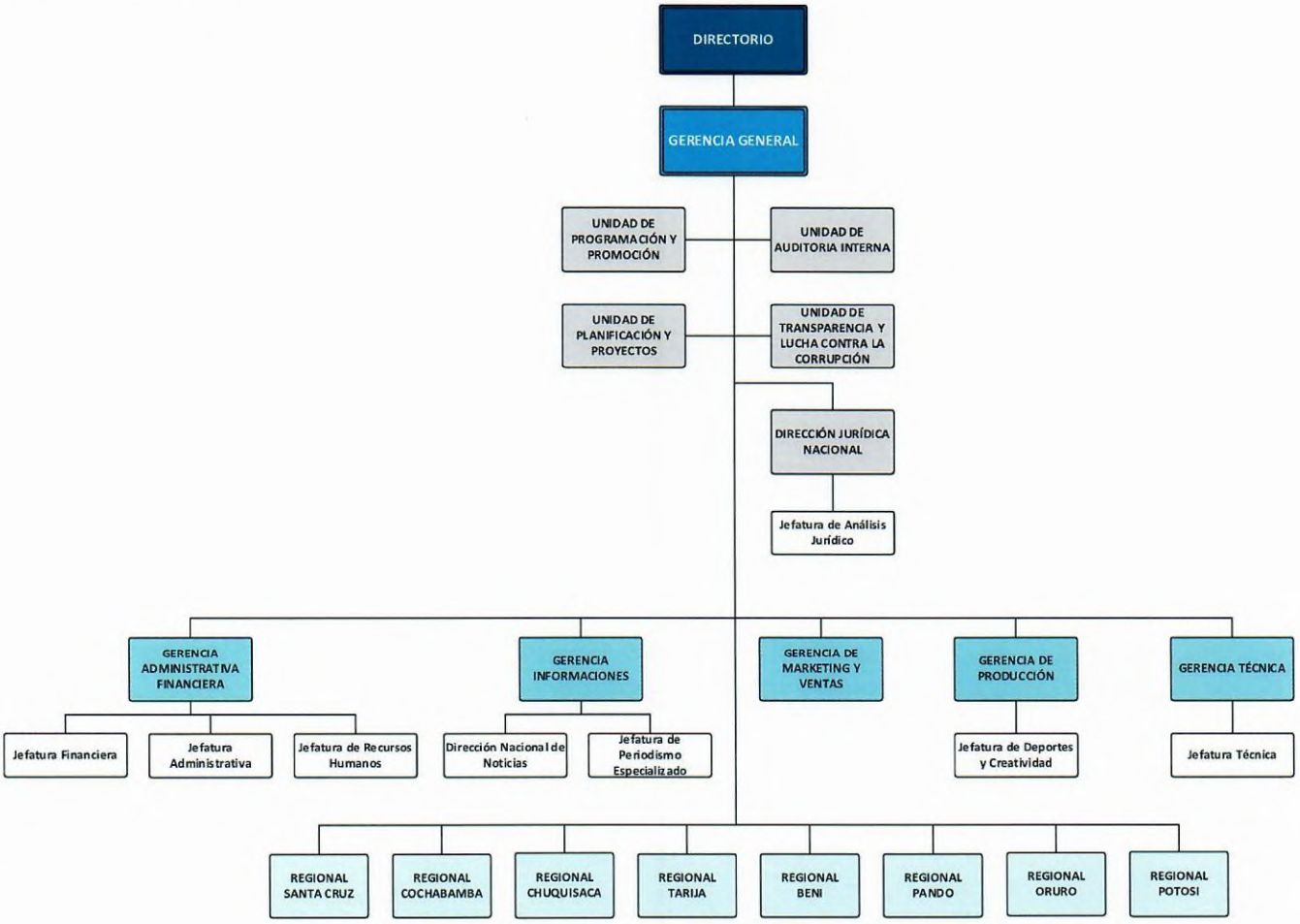
4. ALCANCE DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

El alcance de la implementación del presente plan se aplica al personal de BOLIVIA TV, tanto de planta, consultor de línea y persona natural que tiene relación contractual con la empresa.

Es aplicable todo activo de información que la organización posea en la actualidad o en el futuro, para protegerlos. La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado conocido por toda la organización basándose en metodologías de mejoramiento continuo, aplicado a todas las áreas organizacionales de BOLIVIA TV.

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:

Diagrama 1. Organigrama vigente de BOLIVIA TV aprobado mediante Resolución Administrativa N°17/2021 de 05 de marzo de 2021.



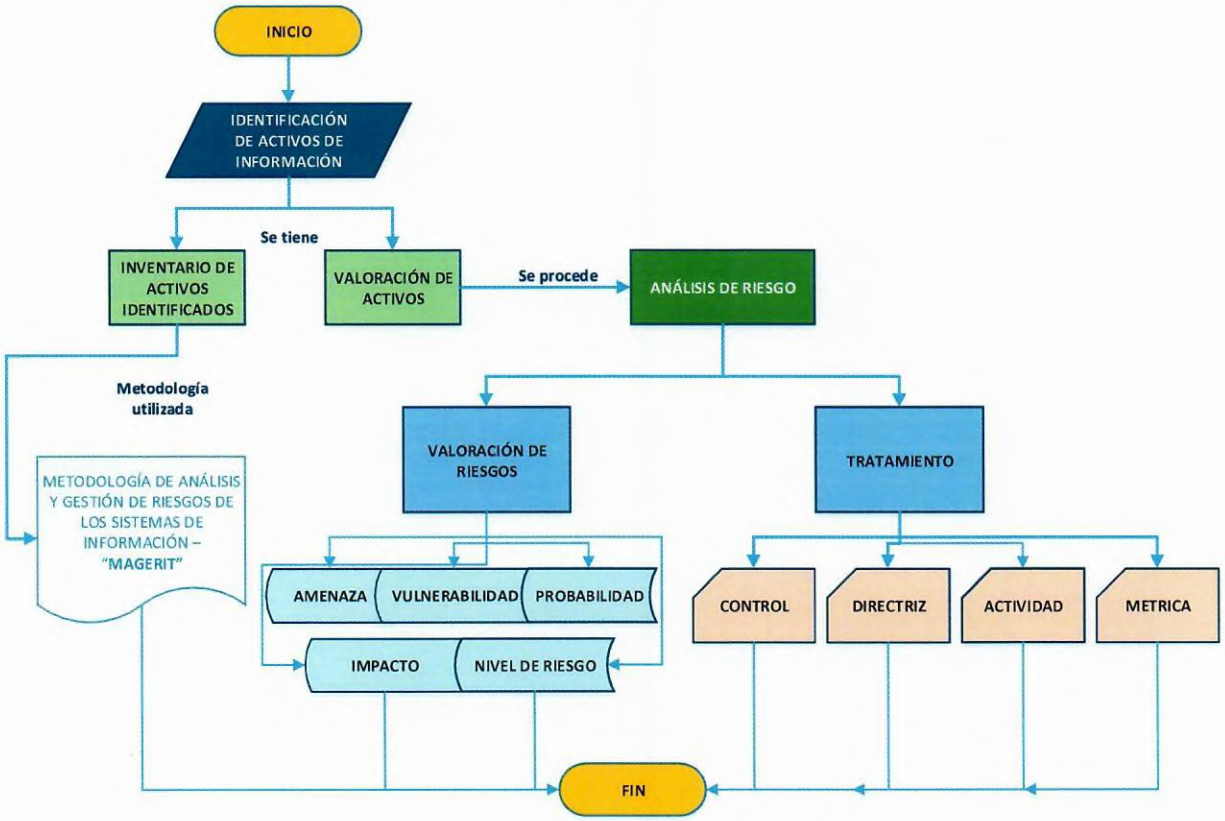
Fuente: Informe Técnico CITE: BTV/UPP/N°016/2021.

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

5. METODOLOGÍA DE GESTIÓN DE RIESGOS

Las metodologías que se utilizan para la elaboración de un PISI, como el caso de la ISO 27001 (norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa) indican que "El eje central es proteger la confidencialidad, integridad y disponibilidad de la información".

Diagrama 2. Diagrama de Valoración de activos fijos y Análisis de Riesgo



Fuente: Elaboración Propia

El PISI contempla la gestión de riesgos en el ámbito de la seguridad de la información. Para esto, se adopta la metodología de gestión de riesgos propuesta dentro de los lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información dentro de BOLIVIA TV, permitiendo identificar las debilidades en cuanto a controles de seguridad inexistentes o ineficaces, y determinar las amenazas y vulnerabilidades asociadas de activos de información.

Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos".

MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Figura 1. Modelo de marco de trabajo para la Gestión de Riesgo



Fuente: ISO 31000 - Marco de Trabajo para la Gestión de Riesgos

5.1. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Los RSI de forma conjunta con los responsables de los procesos identificados dentro del alcance del Plan Institucional de Seguridad de la Información, coordinó el proceso de identificación, clasificación y valoración de activos de información, haciendo uso de la guía incluida en el Anexo B de los Lineamentos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.

La identificación determina qué activos de información formarán parte del PISI haciendo uso de una clasificación.

La valoración de activos de información tiene como objetivo asegurar que la información asociada a los mismos reciba niveles de protección adecuados.

Se valorará los activos de la información en las dimensiones que requiere la institución (Disponibilidad, Integridad y Confidencialidad).

La valoración presenta una escala para la valoración cuantitativa de las características del activo de información.

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
1	Equipo Nube	Equipo encargado de almacenamiento de videos, archivos y medios digitales. Dependiente del servicio de nube, funcionando 24/7.	Soportes de información	En los ambientes del 6 piso en control	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	MUY ALTO	5	ALTO	4	4	ALTO
2	Servicio de internet	Servicio proporcionado por un proveedor ISP	Servicios	En los ambientes de centro de datos - sistemas 6 piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	MUY ALTO	5	ALTO	4	ALTO	4	4	ALTO
3	Página WEB	Sistema de mostrar contenido publicado por la Empresa Estatal de Televisión "BOLIVIA TV"	Datos o Información	En los ambientes de centro de datos - sistemas 6 piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	MUY ALTO	5	MUY ALTO	5	MUY BAJO	1	3	MEDIO
4	Servicio Web	Contempla todas las páginas Web de la empresa BOLIVIA TV.	Claves criptográficas	Quinto y Sexto piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	ALTO	4	MEDIO	3	3	MEDIO
5	TV Online	Servicio de emisión enviado a través de internet de las señales 7,1 y 7,2	Servicios	En los ambientes de centro de datos - sistemas 6 piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	ALTO	4	MUY BAJO	1	3	MEDIO

VoBo. Elaborado/Actualizado por:

VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
6	TV online para celulares (Android)	Servicio de emisión de las señales 7,1 y 7,2 a través de las APP (Android).	Servicios	En los ambientes de centro de datos - sistemas 6 piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	ALTO	4	MUY BAJO	1	3	MEDIO
7	Correo Electrónico Institucional	Correo electrónico institucional, por el cual se realiza el envío e intercambio de información en la empresa y otras instituciones.	Datos o Información	En los ambientes de centro de datos - sistemas 6 piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	ALTO	4	MUY ALTO	5	4	ALTO
8	BD Facturador, BD Squid	1. Equipo encargado de administrar la Base de Datos de los clientes a través un software dedicado a la facturación. 2, Equipo encargado del almacenamiento de información de la catalogación de videos.	Datos o Información	Equipo instalado en el 6 piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	MUY ALTO	5	MUY ALTO	5	4	ALTO
9	Sistema de Correspondencia	Encargado de administrar, difundir correspondencia de la empresa e instituciones externas.	Datos o Información	Equipo instalado en el 6 piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	ALTO	4	MEDIO	3	3	MEDIO

VoBo. Elaborado/Actualizado por:

VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
10	Restream Encoder transmisiones Presidenciales (youtube)	Servicio de Restream (difusión) por el cual se envía contenido audiovisual hacia las redes sociales: facebook, twitter, youtube entre otros. Equipo por el cual se envía información de las transmisiones presidenciales.	Hardware – Equipamiento informático	En los ambientes de centro de datos - sistemas 6 piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	ALTO	4	MEDIO	3	3	MEDIO
11	Servidor NAS de ALMACENAMIENTO	Equipo encargado de almacenar información audiovisual de las áreas: Gerencia de Informaciones, Unidad de Programación y Promoción, Gerencia de Producción y sustantivas.	Datos o Información	Equipo instalado en el 6 piso en el CPD	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	MUY ALTO	5	MUY ALTO	5	ALTO	4	4	ALTO
12	Ingestas (Almacenamiento masivo de señales audiovisuales) y Testigo 7,1	Equipos encargados de recibir señales audiovisuales y almacenarlas.	Datos o Información	Equipos ubicados en el 6to Piso - Sala de Ingestas	GERENCIA DE INFORMACIONES	GERENCIA DE INFORMACIONES	Post-Productores de Informaciones.	MUY ALTO	5	ALTO	4	ALTO	4	4	ALTO

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
13	Equipos de Emisión (Play Out, Servidor Squid, Expresion (Generador de Caracteres))	Equipo encargado de la reproducción de las señales audiovisuales de acuerdo a la escaleta de programación de forma manual o automática en la emisión diaria de BOLIVIA TV.(Squid) Encargado de almacenar contenidos audiovisuales para su emisión. CG. generar y mostrar un texto, dibujo o leyendas en la programación diaria.	Software – Aplicaciones informáticas	Instados en el 6 piso y 5 piso en los controles centrales	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Operadores de VCR	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO
14	Hi - Vision	Equipo de comunicación para transmitir señales audiovisuales, bajo el protocolo SRT.	Redes de comunicaciones	Equipo instalado en el 4 piso	SISTEMAS TELEVISIVOS	Responsable de Generación de Señal	Jheremy Cantuta	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO
15	Servidor NoC	Equipo encargado de realizar mediciones remotas del funcionamiento de los equipos transmisores de las Estaciones Repetidoras, a través de las unidades remotas FLEX, para su supervisión y monitoreo.	Redes de comunicaciones	Equipo instalado en el 6 piso	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	ALTO	4	ALTO	4	4	ALTO

VoBo. Elaborado/Actualizado por:

VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
16	Router Wi-FI	Dispositivo de comunicaciones que permite la configuración de redes: red local y wifi	Hardware – Equipamiento informático	Equipo instalado en los diferentes ambientes	SISTEMAS TELEVISIVOS	Responsable de Sistemas Televisivos	Henry Velez	ALTO	4	MUY ALTO	5	MEDIO	3	4	ALTO
17	Acapella (ROUTER 16X16)	Equipo encargado enrutar y administrar varias señales en formato Full HD para su distribución. El enrutador se encuentra instalado en Planta de Transmisión El Alto en la sala de monitoreo donde se controla el enrutamiento de las señales de la unidades móviles nacionales y transmisiones a nivel internacional	Hardware – Equipamiento informático	En los ambientes de control central pisos 4, 5 y 6 de la Av. Camacho y la Estación Terrena de la Planta El Alto.	Gerencia Técnica	GERENCIA TECNICA	Técnicos de Transmisión, Generación y Sistemas.	ALTO	4	ALTO	4	MEDIO	3	3	MEDIO

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
18	Tablero Eléctrico	Dispositivos eléctricos encargados de la distribución en el suministro de energía eléctrica a las distintas áreas de trabajo, se encuentra instalado en Planta de Transmisión El Alto, donde brinda la energía a la Sala de Transmisión, sala de monitoreo, sala de energía y protección y oficinas de la Planta.	Equipamiento auxiliar	En los ambientes de control central pisos 4, 5 y 6 de la Av. Camacho y la Estación Terrena de la Planta El Alto.	Gerencia Técnica	TECNICO DE SISTEMAS ELECTRICOS E INFRAESTRUCTURA	Franz Lliully Chipana	ALTO	4	ALTO	4	ALTO	4	4	ALTO
19	UPS (Sistema de almacenamiento ininterrumpido)	Equipo encargado de almacenar, estabilizar y suministrar energía eléctrica de manera ininterrumpida, se encuentra instalado en Planta de Transmisión El Alto, en un ambiente dedicado para su almacenamiento.	Equipamiento auxiliar	En los ambientes de control central pisos 4, 5 y 6 de la Av. Camacho y la Estación Terrena de la Planta El Alto.	Gerencia Técnica	GERENCIA TECNICA	Técnicos de Transmisión, Generación y Sistemas.	MUY ALTO	5	ALTO	4	ALTO	4	4	ALTO

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
20	Decoder (HMR)	Se encargan de la Recepción Satelital, ahí es donde se selecciona los niveles de recepción con los datos de los parámetros dependiendo del satélite, este equipo se encuentra en Planta El Alto en la sala de monitoreo.	Redes de comunicaciones	Planta de Transmisión Terrena El Alto	Gerencia Técnica	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	ALTO	4	ALTO	4	ALTO	4	4	ALTO
21	Equipos de monitoreo y medida: monitor forma de onda, vectoroscopio, monitor de audio y analizador de espectro.	Se encargan de monitorear la señal de audio y video, asimismo, los niveles de intensidad que llegan. Esto para verificar el estado de la señal audiovisual al momento de realizar la recepción, el equipo se encuentra en Planta de Transmisión El Alto en la sala de monitoreo	Equipamiento auxiliar	Planta de Transmisión Terrena El Alto	Gerencia Técnica	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	ALTO	4	ALTO	4	ALTO	4	4	ALTO
22	Multiplexor	Se encarga de conversión de las señales TS a una señal BTS para ser inyectado en un Transmisor, se encuentra instalado en la Planta de Transmisión El Alto, en la sala de Transmisión.	Hardware – Equipamiento informático	Planta de Transmisión Terrena El Alto	Responsable Transmisión	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
23	Modulador Satelital	Permite modular la señal ASI y convertirlos en señal TS para adaptarse a cualquier arquitectura de Sistemas, es importante la modulación porque es la señal que se transmitirá, se encuentra instalado en la Planta de Transmisión El Alto, en la sala de Transmisión.	Redes de comunicaciones	Planta de Transmisión Terrena El Alto	Responsable Transmisión	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO
24	Uplink (Antena Satelital)	Se encarga de transportar la señal de enlace de subida (Uplink) para transporte de audio y video como cobertura en todo el territorio Nacional Boliviano e Internacional según la pisada satelital TK, se encuentra instalado en la Planta de Transmisión El Alto, para subir la señal a nivel nacional	Equipamiento auxiliar	Planta de Transmisión Terrena El Alto	Responsable Transmisión	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
25	Pararrayos(Franklin) y Sistema de Tierra	Terminal externo instalado en la torre de transmisión con la función principal de atraer el rayo para tener un punto de impacto controlado e impedir que impacte en los equipos de transmisión, se encuentra instalado en la Planta de Transmisión El Alto, en las Torres Analógico y Digital.	Equipamiento auxiliar	Planta de Transmisión Terrena El Alto	Responsable Transmisión	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO
26	Transformador Reductor	Permite disminuir la tensión de corriente alterna, convierte la tensión 220v a 110 v, se encuentra instalado en la Planta de Transmisión El Alto, en la sala de transmisión.	Equipamiento auxiliar	Planta de Transmisión Terrena El Alto	Responsable Transmisión	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO
27	Supresor de Transientes (LEA)	Es un supresor de picos capaz de eliminar los transientes de voltaje en una línea eléctrica y permite la protección de equipos, se encuentra instalado en la Planta de Transmisión El Alto, en la sala de energía.	Equipamiento auxiliar	Planta de Transmisión Terrena El Alto	Responsable Transmisión	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
28	Transmisor Digital	Equipo encargado de la emisión la señal audiovisual en formato Full HD, bajo el estándar ISDB-Tb, cuenta con diferentes datos de configuración, emite la cobertura a las ciudades de La Paz y El Alto se encuentra instalado en la Planta de Transmisión El Alto, en la sala de Transmisión.	Redes de comunicaciones	Planta de El Alto	Responsable Transmisión	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	MUY ALTO	5	ALTO	4	MUY ALTO	5	4	ALTO
29	Transmisor Analógico	Equipo encargado de la emisión la señal audiovisual bajo la norma NTSC-M, emite la cobertura a las ciudades de La Paz y El Alto, se encuentra instalado en la Planta de Transmisión El Alto, en la sala de Transmisión.	Redes de comunicaciones	Planta de El Alto y Estaciones Repetidoras	Responsable Transmisión	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	MUY ALTO	5	ALTO	4	ALTO	4	4	ALTO

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
30	HPA UP LINK (SATELITAL)	Amplificador de Alta Potencia encargada de realizar la conversión de banda L a banda C o KU para la transmisión satelital, dependiendo de tipo de señal que se tendrá se debe convertir la banda, se encuentra instalado en la Planta de Transmisión El Alto, en la sala de Transmisión, para subir la señal a nivel nacional	Redes de comunicaciones	Planta de El Alto y Unidades Móviles	Responsable Transmisión	Encargado de Planta	Jaime Reynaldo Añaguaya Martinez	MUY ALTO	5	MUY ALTO	5	ALTO	4	4	ALTO
31	Cámaras de video broadcast (6 estudio 6º piso, 9 estudio Robótica)	Equipo para generar señales audiovisuales digitales.	Hardware – Equipamiento informático	Ubicadas y asignadas a los camarógrafos para la grabación de su señal	PRODUCCION	Gerencia de Producción	Operaciones	MUY ALTO	5	ALTO	4	BAJO	2	3	MEDIO
32	Cámaras de video broadcast Streaming (5 z190, 4 x180, total 9)	Equipo para grabar señales digitalmente además de poder transmitir señal hacia el server mediante internet	Hardware – Equipamiento informático	Ubicadas y asignadas a los camarógrafos para la grabación	INFORMACIONES	Gerencia de Informaciones	Camarógrafo de prensa	MUY ALTO	5	ALTO	4	BAJO	2	3	MEDIO

VoBo. Elaborado/Actualizado por:

VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
				de su señal											
33	Mesa de Video (Procesador)	Equipo encargado de administrar varias fuentes de video.	Hardware – Equipamiento informático	Equipo instalado en ambientes del 5 y 6 piso de la Av. Camacho y el Estudio de la Planta El Alto	PRODUCCION	Gerencia de Producción	Operaciones	ALTO	4	MEDIO	3	MEDIO	3	3	MEDIO

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
34	Mesa de Audio	Equipo encargado de administrar varias señales de audios	Hardware – Equipamiento informático	Equipo instalado en ambientes del 5 y 6 piso de la Av. Camacho y el Estudio de la Planta El Alto	PRODUCCION	Gerencia de Producción	Operaciones	ALTO	4	MEDIO	3	MEDIO	3	3	MEDIO
35	Sistema de intercomunicación	Para brindar comunicación en tiempo real y de manera continua entre control central y operadores de cámara.	Hardware – Equipamiento informático	Equipo instalado en ambientes del 5 y 6 piso de la Av. Camacho y el Estudio de la Planta El Alto	Gerencia Técnica	Resp. Generación de Señal	Jheremy Cantuta	MEDIO	3	MEDIO	3	MEDIO	3	3	MEDIO

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
36	CCU Unidad de Control de Camara (6 estudio 6º piso, 9 estudio Robotica)	Equipo encargado del interfaz entre la cámara de video y el switcher de video, por el cual proporciona señales de entrada y salida de video, intercomunicación, señalización (tally).	Hardware – Equipamiento informático	Equipos instalados en los Estudios de televisión y las Unidades Móviles	Gerencia Técnica	Resp. Generación de Señal	Jheremy Cantuta	ALTO	4	ALTO	4	MUY ALTO	5	4	ALTO
37	Router Final FOR-A audio/video	Gestiona y Administra el flujo final de señales de audio/video para nuestro principal destino de envío	Hardware – Equipamiento informático	Control final 6to piso	Gerencia Técnica	Resp. Generación de Señal	Jheremy Cantuta	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO
38	Fibra Óptica (Dataland) estudio central Camacho - Planta El Alto	Medio de transporte de la señal, para enviar y recibir información audiovisual, datos hacia la Planta de El Alto, ABE para su transmisión.	Redes de comunicaciones	Equipos instalados en control central 6 Piso	Gerencia Técnica	Alta Frecuencia	Jaime Añahuaya	ALTO	4	ALTO	4	MEDIO	3	3	MEDIO
39	Router Ross Xtreme audio/video	Gestiona y administra todo el flujo de señales de audio/video que ingresa y salen del control principal multimedia	Hardware – Equipamiento informático	Control principal Sala Multimedia 4to piso	Gerencia Técnica	Resp. Generación de Señal	Jheremy Cantuta	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
40	Switcher Sony audio/video VCR 7,1	Equipo encargo de concentrar las señales de nuestros diferentes estudios y regionales, para posteriormente entregar una señal única a el router grass valley VCR 7,1	Hardware – Equipamiento informático	Control VCR 7.1	Programación	Responsable de Programación	Operador VCR 7,1	ALTO	4	ALTO	4	MUY ALTO	5	5	MUY ALTO
41	Master Control audio/video VCR 7,2	Equipo encargo de concentrar las señales de nuestros diferentes estudios y regionales, para posteriormente entregar una señal única a el router grass valley VCR 7,2	Hardware – Equipamiento informático	Control VCR 7.2	Programación	Responsable de Programación	Operador VCR 7,2	ALTO	4	ALTO	4	ALTO	4	4	ALTO
42	Sistema de monitoreo de video	Conformado por televisores y monitores broadcast, instalados en los controles centrales de estudios, sala VCR 7.1, sala VCR 7.2, sala de ingestas y sala multimedia	Hardware – Equipamiento informático	instalados en 4to, 5to y 6to piso	Gerencia Técnica	Resp. Generación de Señal	Jheremy Cantuta	MEDIO	3	MEDIO	3	MEDIO	3	3	MEDIO
43	Sistema de monitoreo de audio	Conformado por parlantes, amplificadores y monitores de audio, instalados en los controles centrales de estudios, sala VCR 7.1, sala VCR 7.2, sala de ingestas y sala multimedia	Hardware – Equipamiento informático	instalados en 4to, 5to y 6to piso	Gerencia Técnica	Resp. Generacion de Señal	Jheremy Cantuta	MEDIO	3	MEDIO	3	MEDIO	3	3	MEDIO

VoBo. Elaborado/Actualizado por:

VoBo. Revisado por:

INVENTARIO DE ACTIVOS IDENTIFICADOS								VALORACIÓN DE ACTIVOS						Criticidad	VALORACION FINAL
#	Activo	Descripción	Tipo	Ubicación	Unidad Responsable	Responsable	Custodio	Disponibilidad		Integridad		Confidencialidad		Cuantitativo	
44	Sistema de refrigeracion (10 Splits de diferentes capacidades)	Conformado por splits de aire acondicionado que sirven para adecuar la temperatura ambiente a lo requerido por los diferentes equipos instalados en todas las salas como ser control final, multimedia, VCR 7.1, VCR 7.2, controles centrales	Equipamiento auxiliar	instalados en 4to, 5to y 6to piso	Gerencia Técnica	Resp. Generación de Señal	Jheremy Cantuta	MUY ALTO	5	MUY ALTO	5	MUY ALTO	5	5	MUY ALTO

VoBo. Elaborado/Actualizado por:

VoBo. Revisado por:

5.2. EVALUACIÓN DE RIESGO

Para la evaluación de riesgo del P.I.S.I se tuvo la identificación, análisis y valoración de los riesgos asociados a los activos de información; donde surgen las amenazas a partir de la existencia de vulnerabilidades, independientemente que comprometa o no a la seguridad de un sistema.



El análisis y valoración de riesgo evalúa las posibles consecuencias de la materialización de una amenaza producto de las vulnerabilidades presentes en los activos de la información.

La priorización está claramente establecida a partir del nivel de riesgo máximo definido previamente en BOLIVIA TV a través del CSI.

AMBITO DE SEGURIDAD/DESCRIPCION	POSTURA INSTITUCIONAL	ESTADO
1. Seguridad en recursos humanos Es necesario establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y la entidad o institución pública con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral.	Se implementarán controles para los servidores públicos y cualquier persona jurídica o natural que tenga un vínculo laboral con la empresa estatal Bolivia TV.	Utiliza
2. Gestión de activos de información Con el fin de preservar la integridad, disponibilidad y confidencialidad de los activos de información, se debe administrar, controlar y asignar responsabilidades en el uso y protección de los mismos.	Se implementarán controles según lo requiera la gestión de activos de información para preservar la integridad, disponibilidad y confidencialidad de los activos de información se debe administrar, controlar y asignar responsabilidades en el uso y protección de los mismos.	No Utiliza
3. Control de accesos Gestionar los accesos a servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario.	Se implementarán controles para la protección de la información mediante accesos a servicios, sistemas y aplicaciones, además de procedimientos para la gestión de acceso remoto a los mencionados anteriormente.	Utiliza
4. Criptografía El uso de técnicas criptográficas aporta mayores niveles de seguridad para proteger la confidencialidad, autenticidad e integridad de la información, además del no repudio y autenticación	Se implementarán controles según se requiera mediante el uso de técnicas criptográficas para proteger la confidencialidad, autenticidad e integridad de la información.	No Utiliza

5. Seguridad física y ambiental Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y critica para la entidad o institución pública, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.	Se implementarán controles para prevenir y controlar el acceso físico no autorizado a instalaciones seguras o criticas de la entidad, además de minimizar el impacto sobre el equipamiento ante amenazas, peligros ambientales y accesos no autorizados.	Utiliza
6. Seguridad de las operaciones Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta.	Se implementarán controles para documentar procedimientos de operación y preservar la disponibilidad de la información sensible y/o critica.	Utiliza
7. Seguridad de las comunicaciones Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos	Se implementarán controles para gestionar y administrar las redes de datos y la información en tránsito por este medio, agregando también controles para la conexión, autenticación y cifrado de estos servicios.	Utiliza
8. Desarrollo, mantenimiento y adquisición de sistemas Establecer requisitos de seguridad para el desarrollo, mantenimiento y adquisición de sistemas que consideren pruebas de seguridad, pruebas de calidad y aceptación para desarrollos internos y externos.	Se establecerán requisitos de seguridad para el desarrollo, mantenimiento y adquisición de sistemas que consideren pruebas de seguridad, pruebas de calidad y aceptación para desarrollos internos y externos de acuerdo a los activos y sus riesgos identificados	No Utiliza
9. Gestión de incidentes de seguridad de la información Establecer mecanismos para la gestión de incidentes en seguridad de la información dentro de la institución o entidad pública para dar continuidad a las operaciones y mejorar los controles de seguridad implementados.	Se implementarán controles de acuerdo a los riesgos de los activos identificados para establecer mecanismos para la gestión de incidentes en seguridad de la información dentro de la institución, dando continuidad a las operaciones y mejorar los controles de seguridad implementados.	No Utiliza

10. Plan de contingencias tecnológicas Implementar un Plan de Contingencias Tecnológicas que permita controlar un incidente de seguridad de la información o una situación de emergencia, minimizando sus consecuencias negativas. Asimismo, deberá determinar sus requisitos para la seguridad de la información ante situaciones adversas.	Se implementarán controles para definir las estrategias, acciones, procedimientos y responsabilidades para minimizar el impacto de una interrupción imprevista de la funciones críticas y conseguir la restauración de las mismas, dentro de los límites de tiempo establecidos.	Utiliza
11. Cumplimiento Asegurar el cumplimiento operativo del Plan Institucional de Seguridad de la Información que conlleva la Política de Seguridad y la documentación resultante de la misma.	Se implementarán controles de acuerdo a las directrices seleccionadas para asegurar el cumplimiento operativo del Plan Institucional del Seguridad de la Información que conlleva la Política de Seguridad y la documentación resultante de la misma.	No Utiliza

Tabla 1. Valoración de Riesgo

VALORACIÓN DE RIESGOS							
#	**Activo**	**Amenaza**	**Situación**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
1	Equipo Nube	Fallas del Sistema Operativo a nivel hardware	El sistema operativo presenta fallas al inicializarse el sistema, ocasionado por daños en el disco duro de inicio.	No tener la disponibilidad de discos duros HDD para su cambio oportuno.	MUY PROBABLE	MODERADO	ALTO
2	Servicio de internet	Intrusión a la Red por un mal uso del internet	Un funcionario descarga música de una página web de internet el cual al reproducirse se ejecuta un código oculto de acceso remoto	No cerrar puertos y/o limitar los accesos hacia los usuario finales	MUY PROBABLE	CRÍTICO	CRÍTICO

VALORACIÓN DE RIESGOS							
#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
3	Pagina WEB	Hacking por cambio de Gobierno. Sufrir ataques de denegación de Servicio	Por un cambio de Gobierno, personas externas a la institución cambian y/o modifican la información de la página web.	No llegar a hardenizar la configuración de las aplicaciones que se utilizan. Malas prácticas de configuración	MUY PROBABLE	SEVERO	ALTO
4	Servicios web	Falta de protección por un protocolo seguro (Https)	No tener cifrado él envió de los datos y actualización de los mismos certificados de protocolo seguro.	Falta de certificados SSL/TTL.	MUY PROBABLE	MODERADO	ALTO
5	TV Online	corte del servicio de streaming de la página web Ausencia de la señal de emisión de BOLIVIA TV en la página web.	No se llegue a pagar en el plazo establecido al proveedor final por el servicio prestado, dejándonos sin poder emitir la señal por internet.	El desembolso para el pago del servicio depende del Ministerio de Economía. No contar con el flujo efectivo.	POCO PROBABLE	SEVERO	MEDIO
6	TV online para celulares (Android)	La aplicación APK sea Hackeada	Acceso a las cuentas de Google Play	No tener un buen resguardo a los accesos a google storage	PROBABLE	SEVERO	ALTO
			Que una persona malintencionada cambie los parámetros de la aplicación APK	No disponer de copias de seguridad de respaldo de la aplicación.	MUY PROBABLE	MODERADO	ALTO
7	Correo Electrónico Institucional	Correos electrónico falsos (Phishing)	Un funcionario malintencionado hurta las credenciales de acceso de un jefe de otra Área o unidad. Una persona externa haciéndose pasar por un funcionario y pidiendo datos sensibles	Tener anotado en un cuaderno o libreta sus accesos a credenciales. No divulgar información de cuentas o accesos a cualquier persona	PROBABLE	MODERADO	MEDIO

VALORACIÓN DE RIESGOS							
#	**Activo**	**Amenaza**	**Situación**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**
8	BD Facturador, BD Squid	Malas prácticas de codificación	Poder acceder a la base de datos mediante inyecciones SQL.	Malas prácticas de configuración	PROBABLE	MODERADO	MEDIO
		Perdida de la Base de Datos	Que los discos duros se lleguen a dañar por tiempo de funcionamiento 24/7	No tener la disponibilidad de cambiar discos duros de forma inmediata (HDD)	MUY PROBABLE	CRÍTICO	CRÍTICO
9	Sistema de Correspondencia	Alteración de los Datos	Un funcionario modifique los datos de gestiones anteriores para salvarse de sus funciones	No tener control de los accesos para la alteración de los datos	MUY PROBABLE	SEVERO	ALTO
10	Restream Encoder transmisiones Presidenciales (YouTube)	Presentar fallas en el ingreso de video SDI() en la difusión de la señal audiovisual.	El equipo llegue a dañarse por tiempo de funcionamiento 24/7	No tener disponibilidad de otra tarjeta de SDI para restablecer la difusión.	POCO PROBABLE	MENOR	BAJO
11	Servidor NAS de ALMACENAMIENTO	Corrupción de datos en la tabla de partición dañado.	Llenado de la capacidad total del disco duro (HDD) con archivos de información utilizada en el día a día	Lentitud en el sistema de almacenamiento, dejando inoperable su funcionamiento.	MUY PROBABLE	CRÍTICO	CRÍTICO
		Llenado del servidor con materiales audiovisuales sin catalogar	Falta de supervisión y/o designación del responsable en para almacenamiento de las grabaciones.	falta de políticas para el almacenamiento	MUY PROBABLE	CRÍTICO	CRÍTICO
		Virus o malware	archivo, contenido audiovisual o de otro tipo, que pueda llegar a infectar, dañar, o destruir información	no tener el control de actualizar periódica de los servicios	PROBABLE	SEVERO	ALTO

VALORACIÓN DE RIESGOS							
#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
12	Ingestas (Almacenamiento masivo de señales audiovisuales) y Testigo 7,1	Perdida de información audiovisual	Eliminación de los archivos contenidos dentro del equipo por personal no autorizado	No tener controles implementados de acceso al equipo	MUY PROBABLE	CRÍTICO	CRÍTICO
13	Equipos de Emisión (Play Out, Servidor Squid, Expresión (Generador de Caracteres))	Sistema operativo corrompido	Fallas en los discos de arranque.	no tener la disponibilidad inmediata de un cambio oportuno.	MUY PROBABLE	CRÍTICO	CRÍTICO
		Respaldos de Software	El equipo se dañe por sectores defectuosos en el disco duro	No contar con imágenes de respaldo o software de instalación para su reposición inmediata	MUY PROBABLE	CRÍTICO	CRÍTICO
14	Hi - Visión	Perdida de conexión Cambio periódicamente la contraseña	Falla de conexión con el proveedor de servicio de internet.	No tener la disponibilidad del otro punto de acceso del servicio de internet de forma inmediata.	POCO PROBABLE	SEVERO	MEDIO
15	Servidor NoC	Daño o pérdida del sistema operativo	Se llegue a desconfigurar y/o la pérdida del sistema operativo	No disponer de forma inmediata de un bakup del sistema operativo	POCO PROBABLE	SEVERO	MEDIO
16	Router Wi-FI	Abuso de privilegios de acceso. Ataque destructivo	Persona con conocimiento que llega a manipula la red	Mejorando la implementación con nuevos algoritmos para redes según vayan saliendo en el tiempo	PROBABLE	CRÍTICO	ALTO

VALORACIÓN DE RIESGOS							
#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
17	Acapella (ROUTER 16X16)	Corte de suministro de energía eléctrica, y tiempo de vida útil del equipo	Corte en el suministro de energía comercial y falla en el sistema de respaldo UPS, además de mala manipulación del equipo	Corte de suministro de energía eléctrica prolongado	PROBABLE	CRÍTICO	ALTO
18	Tablero Eléctrico	Descargas atmosféricas, variaciones de tensión.	Fallas en el suministro de energía comercial y en el sistema de respaldo UPS	Corte de suministro de energía eléctrica prolongado y descargas atmosféricas	PROBABLE	CRÍTICO	ALTO
19	UPS (Sistema de almacenamiento ininterrumpido)	Corte de suministro de energía eléctrica y Falla en las baterías	Daño en equipo físico, descargas atmosféricas, vida útil de las baterías	Corte de suministro de energía eléctrica prolongado y no prever el mantenimiento en el equipo y no contar con baterías en stock.	PROBABLE	CRÍTICO	ALTO
20	Decoder (HMR)	Corte de suministro de energía eléctrica, modificación de configuración y tiempo de vida útil del equipo	Corte en el suministro de energía comercial y falla en el sistema de respaldo UPS, además de mala manipulación del equipo	Corte de suministro de energía eléctrica prolongado y no prever el mantenimiento en el equipo	PROBABLE	SEVERO	ALTO
21	Equipos de monitoreo y medida: monitor forma de onda, vectoros copio, monitor de audio	Corte de suministro de energía eléctrica, modificación de configuración, actualización de licencias y tiempo de	Corte en el suministro de energía comercial y falla en el sistema de respaldo UPS, además de mala manipulación del equipo	Corte de suministro de energía eléctrica prolongado y no prever el mantenimiento en el equipo	PROBABLE	SEVERO	ALTO

VALORACIÓN DE RIESGOS							
#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
	y analizador de espectro.	vida útil del equipo					
22	Multiplexor	Corte de suministro de energía eléctrica, modificación de configuración, actualización de licencias y tiempo de vida útil del equipo	Corte en el suministro de energía comercial y falla en el sistema de respaldo UPS, además de mala manipulación del equipo	Corte de suministro de energía eléctrica prolongado, no prever mantenimientos respectivos periódicos, tiempo de vida útil	MUY PROBABLE	CRÍTICO	CRÍTICO
23	Modulador Satelital	Corte de suministro de energía eléctrica, modificación de configuración, actualización de licencias y tiempo de vida útil del equipo	Corte en el suministro de energía comercial y falla en el sistema de respaldo UPS, además de mala manipulación del equipo	Corte de suministro de energía eléctrica prolongado, no realizar los mantenimientos respectivos periódicos., tiempo de vida útil y falta de actualización del software	MUY PROBABLE	CRÍTICO	CRÍTICO
24	Uplink (Antena Satelital)	Factores climatológicos e interferencia solar	Cambios climatológicos e interferencias solares	Condiciones meteorológicas extremas (nevadas, granizo, lluvias torrenciales)	MUY PROBABLE	CRÍTICO	CRÍTICO
25	Pararrayos(Franklin) y Sistema de Tierra	Descargas atmosféricas	Temporada de lluvia	Falta de Mantenimiento y tratamiento sistema de tierra	MUY PROBABLE	CRÍTICO	CRÍTICO

VALORACIÓN DE RIESGOS							
#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
26	Transformador Reductor	Descargas atmosféricas, variaciones de tensión.	Fallas en el suministro de energía comercial y en el sistema de respaldo UPS	No prever el mantenimiento en el tablero	PROBABLE	SEVERO	ALTO
27	Supresor de Transcientes (LEA)	Descargas atmosféricas, variaciones de tensión.	Fallas en el suministro de energía comercial	No prever el mantenimiento preventivo en el tablero	PROBABLE	SEVERO	ALTO
28	Transmisor Digital	Corte de suministro de energía eléctrica, modificación de configuración, actualización de licencias y tiempo de vida útil del equipo	Corte en el suministro de energía comercial y falla en el sistema de respaldo UPS, deterioro de los componentes internas del equipo	Corte de suministro de energía eléctrica prolongado, no prever el mantenimiento en el equipo, tiempo de vida útil del equipo, y no contar con equipo de respaldo.	MUY PROBABLE	CRÍTICO	CRÍTICO
29	Transmisor Analógico	Corte de suministro de energía eléctrica, modificación de configuración y tiempo de vida útil del equipo	Corte en el suministro de energía comercial y falla en el sistema de respaldo UPS, deterioro de los componentes internas del equipo	Corte de suministro de energía eléctrica prolongado, no prever el mantenimiento en el equipo, tiempo de vida útil del equipo, y no contar con equipo de respaldo.	MUY PROBABLE	CRÍTICO	CRÍTICO
30	HPA UP LINK (SATELITAL)	Corte de suministro de energía eléctrica, modificación de configuración, y tiempo de vida útil del equipo	Corte en el suministro de energía comercial y falla en el sistema de respaldo UPS, además de mala manipulación del equipo	Corte de suministro de energía eléctrica prolongado, no prever el mantenimiento en el equipo, tiempo de vida útil del equipo.	MUY PROBABLE	CRÍTICO	CRÍTICO

VALORACIÓN DE RIESGOS							
#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
31	Cámaras de video broadcast (6 estudio 6° piso, 9 estudio Robótica)	Daños en el cable que comunica el equipo con la CCU	Mala manipulación por parte del operador de cámara, desgaste natural por tiempo de vida útil.	Desconocimiento del manejo adecuado en cuanto se refiere a la manipulación de los cables de cámara ya sea de naturaleza triaxial o fibra óptica	MUY PROBABLE	MENOR	MEDIO
32	Cámaras de video broadcast Streaming (5 z190, 4 x180, total 9)	Daños en el modem o inestabilidad en la red telefónica que provee el servicio de internet.	Intentar transmitir en lugares donde no existe buen servicio y acceso a la red telefónica	Modem con daño físico o electrónico, mala cobertura de red 4G LTE	MUY PROBABLE	SEVERO	ALTO
33	Mesa de Video (Procesador)	Perdida o cambios en la configuración	Mala manipulación, reseteo accidental	No contar con un respaldo de la configuración	POCO PROBABLE	SEVERO	MEDIO
34	Mesa de Audio	Perdida o cambios en la configuración	Mala manipulación, reseteo accidental	No contar con un respaldo de la configuración	PROBABLE	SEVERO	ALTO
35	Sistema de intercomunicación	Daños en el cable físico que comunica la estación principal (main) con las remotas.	Desperfectos en el cable por el tiempo de vida útil.	No contar con un respaldo de la configuración	POCO PROBABLE	MODERADO	BAJO

VALORACIÓN DE RIESGOS							
#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
36	CCU Unidad de Control de Cámara (6 estudio 6° piso, 9 estudio Robótica)	Fallas de funcionamiento por mala refrigeración.	Daños en el sistema de refrigeración del control central.	No realizar los mantenimientos respectivos periódicos.	PROBABLE	MODERADO	MEDIO
37	Router Final FOR-A audio/video	Corte en el suministro de energía eléctrica, dando lugar a la modificación o perdida de configuración	Corte en el suministro de red eléctrica y fallas en el sistema de respaldo	Corte de suministro de energía eléctrica sea demasiado prolongado.	POCO PROBABLE	CRÍTICO	MEDIO
38	Fibra Óptica (Datalan d) estudio central Camacho - Planta El Alto	Corte del servicio.	por daños en el cableado externo provisto por la empresa datalan	no contar con soporte inmediato ante daños extremos en su cableado	PROBABLE	CRÍTICO	ALTO
39	Router Ross Xtreme audio/video	Corte en el suministro de energía eléctrica, dando lugar a la modificación o perdida de configuración	corte en el suministro de red eléctrica y fallas en el sistema de respaldo	Que el corte de suministro de energía eléctrica sea demasiado prolongado	POCO PROBABLE	CRÍTICO	MEDIO

VALORACIÓN DE RIESGOS							
#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
40	Switcher Sony audio/video VCR 7,1	Corte en el suministro de energía eléctrica, dando lugar a la modificación o perdida de configuración	corte en el suministro de red eléctrica y fallas en el sistema de respaldo	que el corte de suministro de energía eléctrica sea demasiado prolongado	POCO PROBABLE	MENOR	BAJO
41	Master Control audio/video VCR 7,2	Corte en el suministro de energía eléctrica, dando lugar a la modificación o perdida de configuración.	corte en el suministro de red eléctrica y fallas en el sistema de respaldo UPS.	que el corte de suministro de energía eléctrica sea demasiado prolongado	POCO PROBABLE	MODERADO	BAJO
42	Sistema de monitoreo de video	Ausencia de señal de video	Daños en el cableado y/o equipos que le proveen señal	Fallas en el cable de video	POCO PROBABLE	MENOR	BAJO
43	Sistema de monitoreo de audio	ausencia de señal de audio	Daños en el cableado y/o equipos que le proveen señal	Fallas en el cable de audio	POCO PROBABLE	MENOR	BAJO
44	Sistema de refrigeración (10 Splits de diferentes capacidades)	Fallas en los compresores	Deterioro total o parcial del compresor	no contar con soporte inmediato con la empresa que brinda servicio de mantenimiento	PROBABLE	CRÍTICO	ALTO

5.3. MATRIZ DE VALORACIÓN DEL RIESGO

PROBABILIDAD						
	Cierta/Inminente					
	Muy Probable		31	1,4	3,9,32	2,8,11,12,13,22,23,24,25,28,29,30
	Probable			7,8,36	6,20,21,26,27,34	16,17,18,19,38,44
	Poco Probable		10,40,42,43	35,41	5,14,15,33	37,39
	Improbable					
		Irrelevante	Menor	Moderado	Severo	Crítico
		IMPACTO				

5.4. TRATAMIENTO DE RIESGO

Se tomaron decisiones acerca de las medidas más apropiadas para el tratamiento del riesgo identificado en BOLIVIA TV; donde implica la toma de decisiones para aceptar, reducir, retener, evitar o transferir riesgos.

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implemented	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
1	6.1.3. Gestión de la capacidad	i. Identificar los recursos críticos e indispensables para las operaciones. ii. Se deberán revisar y eliminar los datos obsoletos almacenados.	Tener disponibilidad inmediata de discos duros.	No	Análisis de riesgos	A considerar a través del proyecto Fase I, Fase II, Fase III	4 discos duros para datacenter	Discos duros adquiridos / discos duros solicitados
2	7.1.3. Seguridad en la red perimetral	i. Implementar controles de seguridad perimetral que protejan la red ante posibles intrusiones.	Realizar pruebas de testeo para asegurar nuestra red (ética Hacking)	No	Análisis de riesgos	SI	un Informe de la calidad de seguridad obtenida.	informes realizados / informes programados
3	7.1.3. Seguridad en la red perimetral	i. Implementar controles de seguridad perimetral que protejan la red ante posibles intrusiones	Realizar un control minucioso de los servidores instalados.	No	Análisis de riesgos	SI	2 reporte por gestion	reporte realizados / reporte programados
4	7.1.3. Seguridad en la red perimetral	vi. Se deberán implementar protocolos de conexión segura	Adquisicion de certificados con actualizaciones reciente	Si	Análisis de riesgos	SI	un actualización de certificados.	Actualizacion obtenida / actualizacion programada
5	10.1.1. Elaboración del plan de contingencias tecnológicas	i. Cada documento operativo debe incluir responsabilidades, procedimientos, funciones e identificación del personal que ejecutará el plan.	La Jefatura Financiera realiza el seguimiento a los pagos por servicios, sin embargo, esta sujeto a la transferencia de recursos por el Ministerio de Economía.	No	Análisis de riesgos	SI	revision trimestral de comprobantes de pago	revision del pago adquirido / revision de pago solicitado
6	6.2.1. Respaldos de información	i. Identificar la información estratégica y clave para el cumplimiento de los objetivos institucionales.	El área de sistemas administrará las credenciales de google play y también se	No	Análisis de riesgos	SI	un Informe anual de cambios realizados en la credencial.	informes realizados / informes programados

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implemented	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
			cambiará periodicamente la contraseña de acceso.					
	6.2.1. Respaldos de informaci ón	v. Se deberá extraer sumas de comprobación a copias de respaldo para preservar la integridad de la información y en caso de ser necesario se deberá cifrar la información para mantener la integridad de la misma.	Almacenar los archivos de configuracion en los servidores de respaldo.	No	Análisis de riesgos	**A considerar a través del proyecto Fase I, Fase II, Fase III**	adquisiscion de un servidor de respaldos	servidor de respaldos adquirido / servidor de respaldos programado
7	3.2.2. Responsa bilidades de los usuarios para la autenticac ión 5.2.2. Escritorio y pantalla limpia	iii. Los servidores públicos deben evitar mantener la información de autenticación en lugares visibles o de acceso fácil para los demás. vii. El usuario propietario de la cuenta de acceso es responsable del uso de la contraseña. ii. Bloquear la pantalla cuando se encuentre sin supervisión	Capacitacion a todo el personal que maneja credenciales sensibles e inherentes a la empresa.	No	Análisis de riesgos	**SI**	1 capacitacion a todos los servidores sobre la utilizacion correcta de las credenciales	Capacitacion realizada / Capacitacion Programada
8	8.1.6. Seguridad en bases de datos	i. Aplicar recomendaciones de configuración en seguridad provistas por el desarrollador del gestor de base de datos. viii. Se deberán optimizar las consultas lógicas a bases de datos.	Realizar pruebas de testeo al servidor de aplicaciones.	No	Análisis de riesgos	**SI**	1 reporte por gestion acerca de la seguridad de la informacion	reporte realizados / reporte programados
	6.1.3. Gestión de la capacidad	i. Identificar los recursos críticos e indispensables para las operaciones.	Disponibilidad inmediata de discos duros	No	Análisis de riesgos	**A considerar a través del proyecto**	8 discos duros para datacenter	discos duros comprados / discos duros solicitados

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implemented	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
						Fase I, Fase II, Fase III		
9	2.2.3. Protección del archivo	ii. Elaborar controles para evitar la modificación y el acceso no autorizado a la información archivada.	Solicitar autorización por la MAE para realizar modificaciones en los destinatarios.	No	Análisis de riesgos	SI	correos electrónicos de autorización por la MAE o quien designe la misma.	autorizaciones atendidas / autorizaciones requeridas
10	6.1.2. Gestión de cambios	iii. Los cambios de configuración deberán considerar el impacto asociado y realizarse en un ambiente controlado.	Compra de tarjeta de video SDI.	No	Análisis de riesgos	SI	2 tarjetas de video SDI	tarjetas de video SDI adquirido / tarjetas de video SDI solicitado
11	6.1.3. Gestión de la capacidad	i. Identificar los recursos críticos e indispensables para las operaciones.	Compra de discos duros para acciones inmediatas de restablecimiento a su normalidad	No	Análisis de riesgos	A considerar a través del proyecto Fase I, Fase II, Fase III	30 discos duros para almacenamiento para datacenter	numero de discos adquiridos/ número total de discos solicitados
	6.2.1. Respaldos de información	i. Identificar la información estratégica y clave para el cumplimiento de los objetivos institucionales.	Creación de políticas de uso de almacenamiento con las áreas de Prensa, Producción, Programación	No	Análisis de riesgos	SI	Política de uso de almacenamiento para evitar la duplicidad o archivos innecesarios	Política implementadas / Política programada
	6.1.2. Gestión de cambios	ii. Los cambios de configuración deberán considerar el impacto asociado y realizarse en un ambiente controlado.	verificar que las actualizaciones estén con las últimas actualizaciones recomendadas	No	Análisis de riesgos	SI	Actualizaciones las más recientes a aprobadas	

VoBo. Elaborado/Actualizado por:

VoBo. Revisado por:

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implementado	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
12	3.2.1. Administración de accesos, cancelación y privilegios de usuarios	i. Se deberán establecer los requisitos de autorización para la creación y asignación de roles y privilegios de una cuenta.	Crear usuarios con privilegios de lectura	No	Análisis de riesgos	**SI**	1) Revisión trimestral de usuarios creados correctamente	Discos duros adquiridos / discos duros solicitados
						SI	2) Compra de (8) discos duros solidos	
13	10.1.1. Elaboración del plan de contingencias tecnológicas	v. La entidad o institución pública deberá identificar los requisitos institucionales para la disponibilidad de los sistemas de información.	Compra de discos duros	No	Análisis de riesgos	**SI**	3 discos duros solidos	Discos duros adquiridos / discos duros solicitados
	6.2.1. Respaldos de información	i. Identificar la información estratégica y clave para el cumplimiento de los objetivos institucionales.	Adquisición de un servidor de respaldo.	No	Análisis de riesgos	**A considerar a través del proyecto Fase I, Fase II, Fase III**	1 copia de respaldo	copia de respaldo realizadas / copias de respaldo programadas
14	7.1.1. Gestión de la red	iii. Considerar la implementación de dispositivos de red redundantes para puntos de fallo único donde la disponibilidad sea un factor crítico.	Disponer de otro punto de acceso de internet con las mismas características de internet principal	No	Análisis de riesgos	**SI**	instalación de un punto de red con las mismas características del principal	instalación realizada / instalación programada
15	6.2.1. Respaldos de información	i. Identificar la información estratégica y clave para el cumplimiento de	Obtener copias de seguridad para enviar al servidor de respaldo	No	Análisis de riesgos	**A considerar a través del proyecto**	1 copia de respaldo	copia de respaldo realizadas / copias de respaldo

	TRATAMIENTO							
#	**Control**	**Directriz**	**Actividad**	**Implementado**	**Justificación Inclusión**	**Por implementar**	**MÉTRICA**	**Indicador**
		los objetivos institucionales.				**Fase I, Fase II, Fase III**		programadas
16	7.1.5. Seguridad en redes WiFi	ii. Concientizar sobre el uso seguro de las redes WiFi, que informe sobre los riesgos de conexión a redes desconocidas y no autorizadas. iv. Filtrar el acceso a la red WiFi por dirección MAC, servidor proxy o cualquier otro método de acuerdo al reglamente de gestión de la red de comunicaciones	Limitar y concientizar al personal de los accesos concedidos y la no divulgación para ataques a la clonación de MAC addres.	No	Análisis de riesgos	**SI**	1 Capacitacion anual al personal que utiliza nuestras redes WI-FI	Capacitación realizada / Capacitación Programada
17	10.1.1. Elaboración del plan de contingencias tecnológicas.	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos.	1. Mantenimiento preventivo a las UPS y verificación del correcto funcionamiento del grupo generador y ATS (Sistema de Transferencia Automática).	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados al sistema de respaldo UPS, Grupo Generador, Cantidad	1. informes realizados / informes programados
			2. Compra de Router de respaldo			**A considerar a través del proyecto Fase I, Fase II, Fase III**	2) Contar con un (1) equipo de respaldo router.	2, respaldo acapela adquirido / respaldo acapela solicitado

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implemented	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
18	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos. iii. Implementar controles para minimizar el impacto ocasionado por condiciones ambientales, incendios, inundaciones, polvo, vibraciones, interferencias eléctricas y otros.	1. Mantenimiento preventivo a las UPS y verificación del correcto funcionamiento del grupo generador 2. Compra de baterías para UPS.	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados al sistema de respaldo UPS, Grupo Generador, sistema de tierra.	1. informes realizados / informes programados
						A considerar a través del proyecto Fase I, Fase II, Fase III	2) Contar con (1) tablero de respaldo de energía eléctrica.	2. tablero instalado / número tablero programado
19	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación	1. Mantenimiento preventivo a las UPS y verificación del correcto funcionamiento del grupo generador	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados al sistema de respaldo UPS, Grupo Generador	1. informes realizados / informes programados

	TRATAMIENTO								
#	Control	Directriz	Actividad	Implemented	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
	equipamiento	de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	2. Compra de baterías			**A considerar a través del proyecto Fase I, Fase II, Fase III**	2) Contar con respaldo de 1 unidad de UPS con su banco de baterías de 40 unidades.	2, respaldo ups con banco de baterías adquirido / respaldo de ups con banco de baterías solicitado
20	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	1. Mantenimiento preventivo de los equipos y verificación del correcto funcionamiento del equipo de respaldo.	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados.	1, Informe realizados / informes programado
						A considerar a través del proyecto Fase I, Fase II, Fase III	. 2) Contar con respaldo de 4 unidades de Decoder (HMR)	2, respaldo de decoder adquirido / respaldo de decoder solicitado

VoBo. Elaborado/Actualizado por:

VoBo. Revisado por:

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implementado	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
21	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticas y los recursos tecnológicos asociados a estos. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	1. Mantenimiento preventivo de los equipos y verificación del correcto funcionamiento del equipo de respaldo.	SI	1. Mantenimiento preventivo de los equipos y verificación del correcto funcionamiento del equipo de respaldo.	**SI**	1) Informes periódicos de los mantenimientos realizados al sistema de respaldo UPS, Grupo Generador.	1, Informe realizados / informes programado
			2. Compra de equipos de monitoreo	SI	2. Compra de equipos de monitoreo	**A considerar a través del proyecto Fase I, Fase II, Fase III**	2) Contar con respaldo de cada uno de los equipos a 1 unidad.	2, respaldo de equipos adquiridos / respaldo de equipos solicitados
22	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1.	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos	1. Mantenimiento preventivo de los equipos y verificación del correcto	SI	Análisis de riesgos	**SI**	1)Informes periódicos de los mantenimientos realizados al equipo.	1, Informe realizados / informes programado

	TRATAMIENTO							
#	**Control**	**Directriz**	**Actividad**	**Implementado**	**Justificación Inclusión**	**Por implementar**	**MÉTRICA**	**Indicador**
	Seguridad del equipamiento	que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	funcionamiento del equipo de respaldo.			**A considerar a través del proyecto Fase I, Fase II, Fase III**	2) Contar con respaldo de 1 unidad de Multiplexor	2, respaldo multiplexor adquirido / respaldo multiplexor solicitado
23	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticas y los recursos tecnológicos asociados a estos. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	1. Mantenimiento preventivo de los equipos y verificación del correcto funcionamiento del equipo de respaldo.	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados al equipo.	1, Informe realizados / informes programado
						A considerar a través del proyecto Fase I, Fase II, Fase III	2) Contar con respaldo de 1 unidad de Modulador Satelital	2, Modulador satelital adquirido / modulo satelital solicitado
24	5.2.1. Seguridad del Equipamiento	iii. Implementar controles para minimizar el impacto ocasionado por condiciones ambientales, incendios, inundaciones, polvo, vibraciones, interferencias eléctricas y otros.	Disponer personal de turno encargada de atender la contingencia climatológica.	SI	Análisis de riesgos	**SI**	Informes ocasionales ante el cambio climatológico .	1, Informe realizados / informes programado

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

	TRATAMIENTO							
#	**Control**	**Directriz**	**Actividad**	**Implemen tado**	**Justificación Inclusión**	**Por implementar**	**MÉTRICA**	**Indicador**
25	5.2.1. Seguridad del Equipamiento	iii. Implementar controles para minimizar el impacto ocasionado por condiciones ambientales, incendios, inundaciones, polvo, vibraciones, interferencias eléctricas y otros. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	Mantenimiento al sistema de aterramiento.	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados al sistema de tierra.	1, Informe realizados / informes programado
						A considerar a través del proyecto Fase I, Fase II, Fase III	2) Contar con un respaldo de 2 unidades de pararrayos y su sistema de tierra	2, respaldo de pararrayos adquiridos / respaldo de pararrayos solicitados
26	5.2.1. Seguridad del Equipamiento	iii. Implementar controles para minimizar el impacto ocasionado por condiciones ambientales, incendios, inundaciones, polvo, vibraciones, interferencias eléctricas y otros. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	1. Mantenimiento preventivo del sistema de tierra	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados al sistema de tierra.	1, Informe realizados / informes programado
27	5.2.1. Seguridad del Equipamiento	iii. Implementar controles para minimizar el impacto ocasionado por condiciones ambientales, incendios, inundaciones, polvo, vibraciones, interferencias eléctricas y otros. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal	1. Mantenimiento preventivo.	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizado.	1, Informe realizados / informes programado

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implementado	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
		calificado al equipamiento de acuerdo a las especificaciones del fabricante.				**A considerar a través del proyecto Fase I, Fase II, Fase III**	2) Contar con respaldo de 1 unidad de Supresor de Transcientes.	2, respaldo de supresor de trancientes adquirido /respaldo de supresor de trancientes solicitados
28	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	1. Mantenimiento preventivo del equipo y verificación del correcto funcionamiento.	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados al equipo.	1, Informe realizados / informes programado
						A considerar a través del proyecto Fase I, Fase II, Fase III	2) Contar con respaldo de (1) unidad de Transmisor Digital.	2, respaldo de transmisor digital adquirido / respaldo de transmisor digital solicitado
29	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los	1. Mantenimiento preventivo del equipo y verificación del correcto funcionamiento.	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados.	1, Informe realizados / informes programados

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implementado	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
	equipamiento	procesos, operaciones críticas y los recursos tecnológicos asociados a estos. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.						
30	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos. v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	1. Mantenimiento preventivo de los equipos y verificación del correcto funcionamiento del equipo de respaldo.	SI	Análisis de riesgos	**SI**	1) Informes periódicos de los mantenimientos realizados.	1, Informe realizados / informes programados
						A considerar a través del proyecto Fase I, Fase II, Fase III	2) Contar con respaldo de (1) unidad de HPA	2. respaldo HPA adquirido / respaldo HPA solicitado
31	1.2.1 Capacitación y formación	ii. Realizar capacitaciones acerca del Plan Institucional de Seguridad de la Información y las Políticas de Seguridad de la Información incluidas, con énfasis en las áreas de desempeño de los servidores públicos a ser capacitados.	Implementación de jornadas de capacitación a los operadores de cámara.	No	Análisis de Riesgos	**SI**	Capacitación realizada	Capacitación realizada/Capacitación Programada
32	1.2.1 Capacitación y formación 7.1.1. Gestión de la red	ii. Realizar capacitaciones acerca del Plan Institucional de Seguridad de la Información y las Políticas de Seguridad de la Información incluidas, con énfasis en las áreas de desempeño de los servidores públicos a ser capacitados. iii. Considerar la implementación de dispositivos de red redundantes para	1. Implementación de jornadas de capacitación a los operadores de cámara.	SI	1. Implementación de jornadas de capacitación a los	**SI**	1) Una Capacitación Anual realizada.	1. Capacitación realizada./ Capacitación Programada

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implementado	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
		puntos de fallo único donde la disponibilidad sea un factor crítico.			operadores de cámara.			
			2. Adquisición de chips de otra empresa telefónica con servicio de internet, adicional con el que se cuenta al momento	SI	2. Adquisición de chips de otra empresa telefónica con servicio de internet, adicional con el que se cuenta al momento	**SI**	2) Adquisición de chips telefónicos con servicio a internet	2. chip adquirido / chip solicitado
			3. Adquisición de Sistema de Transmisión y recepción IP (Mochila de transmisión)	SI	3. Adquisición de Sistema de Transmisión y recepción IP (Mochila de transmisión	**SI**	1) Adquisición de la mochila	3. Mochila adquirida/Mochila solicitada
33	1.2.1 Capacitación y formación 6.2.1 Seguridad de las operaciones	ii. Realizar capacitaciones acerca del Plan Institucional de Seguridad de la Información y las Políticas de Seguridad de la Información incluidas, con énfasis en las áreas de desempeño de los servidores públicos a ser capacitados. 6.2.1.viii. En caso de tratarse de información crítica y/o estratégica se deberán almacenar los respaldos en múltiples medios de acuerdo a requerimiento.	Implementación de jornadas de capacitación a los operadores de video. Implementación de mantenimientos preventivos programados.	No	Análisis de Riesgos	**SI**	Capacitación realizada. Mantenimiento realizado.	Capacitación realizada / Capacitación Programada
34	1.2.1 Capacitación y formación	ii. Realizar capacitaciones acerca del Plan Institucional de Seguridad de la Información y las Políticas de Seguridad de la Información incluidas, con énfasis en las áreas de desempeño de los servidores públicos a ser capacitados.	Implementación de jornadas de capacitación a los operadores de sonido. Implementación de	No	Análisis de Riesgos	**SI**	Capacitación realizada. Mantenimiento realizado.	Capacitación realizada / Capacitación Programada

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implemented	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
			mantenimientos preventivos programados.					
35	1.2.1 Capacitación y formación	ii. Realizar capacitaciones acerca del Plan Institucional de Seguridad de la Información y las Políticas de Seguridad de la Información incluidas, con énfasis en las áreas de desempeño de los servidores públicos a ser capacitados.	Implementación de jornadas de capacitación a los operadores de video, sonido, VCR 7.1 y VCR 7.2.	No	Análisis de Riesgos	**SI**	Capacitación realizada	Capacitación realizada / Capacitación Programada
36	5.3.1. Condiciones operativas	x. Se deberá implementar dispositivos de enfriamiento y extracción de aire.	Realizar mantenimientos periódicos al sistema de refrigeración.	No	Análisis de Riesgos	**SI**	Informes de mantenimientos.	mantenimientos realizados / Mantenimientos programados
37	10.1.1. Elaboración del plan de contingencias tecnológicas 6.2.1 Seguridad de las operaciones	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticos y los recursos tecnológicos asociados a estos. 6.2.1. viii. En caso de tratarse de información crítica y/o estratégica se deberán almacenar los respaldos en múltiples medios de acuerdo a requerimiento.	1. Mantenimiento preventivo a las UPS y verificación del correcto funcionamiento del grupo generador de energía eléctrica.	SI	Análisis de riesgos	**SI**	1. Informes periódicos de los mantenimientos realizados al sistema de respaldo.	1. Mantenimientos realizados / mantenimientos programados

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implemented	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
			2. Compra de repuestos para UPS en stock (UPS sala control final) 3. Mantenimiento programados.			SI	2. compra de 60 baterías (12v 9Ah)	2. baterías compradas / baterías solicitadas
38	7.1.1. Gestión de la red	iii. Considerar la implementación de dispositivos de red redundantes para puntos de fallo único donde la disponibilidad sea un factor crítico.	Asegurarse de que los contratos del proveedor de servicios incluyan requisitos de seguridad, con los servicios de comunicación vía Fibra Óptica. Solicitar los servicios de otra empresa para el servicio de fibra óptica.	NO	Análisis de Riesgo	SI	Servicio fibra óptica con su respaldo.	Servicio Adquirido / Servicio Solicitado
39	10.1.1. Elaboración del plan de contingencias tecnológicas 6.2.1 Seguridad de las operaciones	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticas y los recursos tecnológicos asociados a estos. 6.2.1. viii. En	1. Mantenimiento preventivo a las UPS y verificación del correcto funcionamiento del grupo generador de energía eléctrica.	SI	Análisis de riesgos	SI	1. Informes periódicos de los mantenimientos realizados al sistema de respaldo.	1. Mantenimientos realizados / mantenimientos programados

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implementado	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
		caso de tratarse de información crítica y/o estratégica se deberán almacenar los respaldos en múltiples medios de acuerdo a requerimiento.						
40	10.1.1. Elaboración del plan de contingencias tecnológicas 6. Seguridad de las operaciones	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticas y los recursos tecnológicos asociados a estos. 6.2.1. viii. En caso de tratarse de información crítica y/o estratégica se deberán almacenar los respaldos en múltiples medios de acuerdo a requerimiento.	1. Mantenimiento preventivo a las UPS y verificación del correcto funcionamiento del grupo generador de energía eléctrica.	SI	Análisis de riesgos	**SI**	1. Informes periódicos de los mantenimientos realizados al sistema de respaldo.	1. Mantenimientos realizados / mantenimientos programados.
41	10.1.1. Elaboración del plan de contingencias tecnológicas 6.2.1 Seguridad de las operaciones	i. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información; la mejora continua a partir de la Gestión de Incidentes de Seguridad de la Información; la determinación de los eventos que afecten la operación de los sistemas de información; la determinación de los procesos, operaciones críticas y los recursos tecnológicos asociados a estos. 6.2.1. viii. En caso de tratarse de información crítica y/o estratégica se deberán	1. Mantenimiento preventivo a las UPS y verificación del correcto funcionamiento del grupo generador de energía eléctrica.	SI	Análisis de riesgos	**SI**	Informes periódicos de los mantenimientos realizados al sistema de respaldo.	1. Mantenimientos realizados / mantenimientos programados.

	TRATAMIENTO							
#	Control	Directriz	Actividad	Implementado	Justificación Inclusión	Por implementar	MÉTRICA	Indicador
		almacenar los respaldos en múltiples medios de acuerdo a requerimiento.						
42	5.2.1. Seguridad del equipamiento	v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	Mantenimientos periódicos	NO	Análisis de Riesgos	SI	Informes de mantenimiento.	Mantenimientos realizados / mantenimientos programados.
43	5.2.1. Seguridad del equipamiento	v. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.	Mantenimientos periódicos	NO	Análisis de Riesgos	SI	Informes de mantenimiento.	Mantenimientos realizados / mantenimientos programados.
44	5.3.1. Condiciones operativas	x. Se deberá implementar dispositivos de enfriamiento y extracción de aire.	Servicio de mantenimiento programado.	NO	Análisis de Riesgos	SI	Informes de mantenimiento.	Mantenimientos realizados / mantenimientos programados.

5.5. CONTROLES MÍNIMOS DE SEGURIDAD DE LA INFORMACIÓN

Los controles de Seguridad de la Información que serán implementados se encuentran referenciados "Controles Implementados y por Implementar" y en el punto de "Desarrollo" de la política de la Seguridad de la Información.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

6.1. OBJETIVO GENERAL

La Política de Seguridad de Información de BOLIVIA TV, tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información generada en los Estudios de televisión y que son procesados

para su difusión, a través de la protección de los activos, operaciones y procesos vinculados con el flujo de información (señal).

6.2. OBJETIVO ESPECIFICO

La Política de Seguridad de Información, 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 la prestación del servicio de televisión, a través de la emisión y reproducción de las señales en todo el territorio boliviano.
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 empresa.
d) Aplicar de manera efectiva los paradigmas de buenas prácticas de seguridad en la generación y transmisión de la información audiovisual, para la generación de políticas necesarias que mitiguen los riesgos de información identificados.
e) Mantener la confidencialidad de la información generada, procesada en los sistemas de almacenamiento internamente y/o por terceros.

6.3. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades definidos para la seguridad de la información de la entidad se describen a continuación.

6.4. DESIGNACIÓN Y RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN

El responsable de la Seguridad de la Información (RSI) será el o la profesional, con perfil y experiencia en gestión de seguridad de la información, designado por la MAE, que tendrá como función principal la elaboración e implementación del PISI.

6.4.1. Funciones del RSI

- 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 la información
- Proponer la Política de Seguridad de la Información (PISI), incorporado dentro del PISI.
- Gestionar el cumplimiento del PISI
- Elaborar manuales de procesos y/o procedimiento de seguridad específicos dentro de los lineamientos del Plan Institucional de Seguridad De Información y promover su difusión en la entidad

- Coordinar la inducción, capacitación y comunicación del personal, en el marco del PISI
- Gestionar y coordinar la atención y respuesta de incidentes 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 entidad.
- 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 del mecanismo de seguridad, que coadyuven a la reducción de los riegos identificados.

Otras funciones que resulten necesarias para preservar la seguridad de la información.

6.5. DESIGNACIÓN Y FUNCIONES DEL COMITÉ DE LA SEGURIDAD DE LA INFORMACIÓN

La Máxima Autoridad Ejecutiva designara al personal que conformara el Comité de Seguridad de la Información (CSI), 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 considera la posibilidad de que estos asuman las funciones del CSI.

El CSI establecerá su organización interna y asumirá 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 procedimientos de seguridad que se desprenden de la Política de Seguridad de la Información incorporada del PISI.
- Proponer estratégicas necesarias para la implementación y 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

6.6. CUSTODIOS DE LOS ACTIVOS DE INFORMACIÓN

- Tomar medidas para minimizar el riesgo por perdida o exposición de los activos de la información que están bajo su responsabilidad
- Realizar el inventario de los activos de información a su cargo
- Identificación, análisis evaluación y tratamiento de riesgo de seguridad de la información
- Autorizar accesos sobre la información de las que son propietarios, ratificar periódicamente estos accesos e informar inmediatamente a las áreas competentes sobre el personal que no debería tener acceso a la misma.
- Revisar y dar conformidad a la matriz de riesgo

Gerente General:

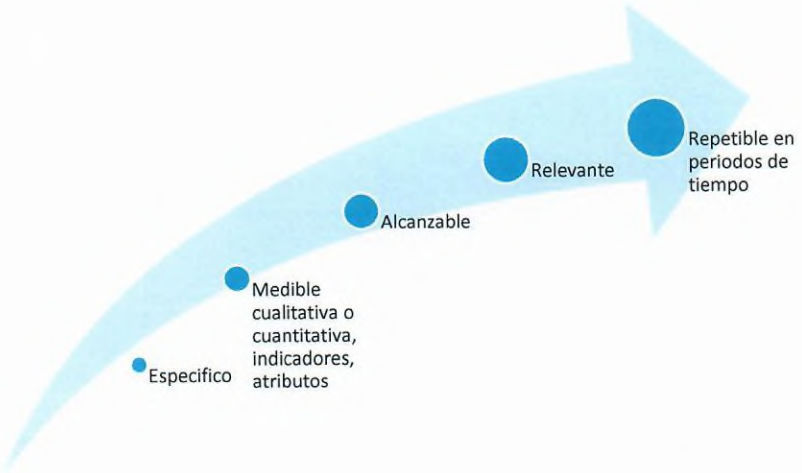
En su calidad de Máxima Autoridad Ejecutiva respecto a la seguridad de la información deberá:

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 09 de septiembre de 2015 y Decreto Supremo N°1793, de 13 de noviembre de 2013, de reglamentación a la Ley 164).
c) Designar al Responsable de Seguridad de la Información (RSI).
d) Conformar el Comité de Seguridad de la Información (CSI).
e) Asegurar que los objetivos y alcances del Plan Institucional de Seguridad de la Información sean compatibles con los objetivos del Plan Estratégico Empresarial.
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.
i) Asumir otras acciones a favor de la seguridad de la información.

6.7. INDICADORES Y METRICAS

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.

Los miembros del RSI establecen los indicadores y métricas de cumplimiento al momento de elaborar y desarrollar un determinado control de seguridad, con la finalidad de evaluar la eficacia de dichos controles una vez que se implementen.



6.8. CUMPLIMIENTO

La presente Política de Seguridad de la Información es de cumplimiento obligatorio para todo servidor público dependiente de BOLIVIA TV y todas sus áreas organizacionales.

A fin de proseguir en la implementación del plan, BOLIVIA TV ha elaborado el Plan Operativo Anual, Anteproyecto de Presupuesto de la gestión 2024, aprobado mediante Resolución de Directorio N°002/2023 de 06 de septiembre de 2023, que establece el presupuesto a ejecutar por cada una de las actividades a desarrollar por cada una de las áreas organizacionales ya sean sustantivas y administrativas, a objeto de dar cumplimiento de las Acciones a Corto Plazo. Para tal efecto, el Anteporyecto de POA y Presupuesto de la gestión 2024 las áreas/instancias organizacionales de BOLIVIA TV (Entidad 526), se ha estructurado la actividad establecida, así como la estructura programática de las áreas/instancias organizacionales que convergen en el cumplimiento de la acción de corto plazo, en la implementación del Plan Institucional de Seguridad de la Información parte del equipamiento y servicios están en las memorias de cálculo del anteproyecto de POA y Presupuesto para la gestión 2024.

7. DIFUSIÓN

La existencia de un Plan de Difusión, capacitación y sensibilización en torno a la seguridad de la información.

El Gerente General de BOLIVIA TV, será el responsable de la existencia permanente y el cumplimiento del PISI, en la capacitación y sensibilización de la seguridad de la información.

El Encargado del Seguridad de Información es el responsable de la ejecución del Plan y el cumplimiento de sus objetivos.

8. SANCIONES

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas y en caso de corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes.

9. HISTORICO DE CAMBIOS

Fecha	Formulario	Estado	Encargado
27/10/2023	Políticas de Seguridad	En revisión	Miembros RSI
31/10/2023	Políticas de Seguridad	Aprobado	Comité BTV

10. CRONOGRAMA DE IMPLEMENTACIÓN

Se elaboró un cronograma de implementación de los controles definidos del Plan Institucional de Seguridad de la Información a continuación:

CRONOGRAMA GESTIÓN 2024

Activos de Información	Plan de Seguridad	Control	Roles y Responsabilidades	Métrica	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Equipo Nube	6. Seguridad de las operaciones	6.1.3. Gestión de la capacidad	Gerencia Administrativa y Financiera. Contrataciones. Sistemas	4 discos duros para datacenter												
Servicio de internet	7. Seguridad de las comunicaciones	7.1.3. Seguridad en la red perimetral	Sistemas	un Informe de la calidad de seguridad obtenida.												

	7. Seguridad de las comunicaciones	7.1.1. Gestión de la red	Contrataciones. Sistemas	Incluir en las especificaciones técnicas punto de acceso redundante o reglas de cumplimiento de la conexión. El cableado principal hasta la acometida en su trayecto no sufra desgaste por fricción.	
Página WEB	7. Seguridad de las comunicaciones	7.1.3. Seguridad en la red perimetral	Sistemas	2 reporte por gestión	
Servicios Web	7. Seguridad de las comunicaciones	7.1.3. Seguridad en la red perimetral	Gerencia Administrativa y Financiera. Contrataciones. Sistemas	una actualización de certificados.	
TV Online	10. Plan de Contingencias Tecnológicas	10.1.1. Elaboración del plan de contingencias tecnológicas	Jefatura Financiera	revisión trimestral de comprobantes de pago	
TV online para celulares (Android)	6. Seguridad de las operaciones	6.2.1. Respaldos de información	Sistemas	un Informe anual de cambios realizados en la credencial.	

Correo Electrónico institucional	3. Control de accesos	3.2.2. Responsabilidades de los usuarios para la autenticación 5.2.2. Escritorio y pantalla limpia	Gerencia Administrativa Finanaciera, Recursos Humanos, Sistemas.	1 capacitación a todos los servidores sobre la utilización correcta de las credenciales	
BD Facturador, BD Squid	8. Desarrollo, mantenimiento y adquisición de sistemas	8.1.6. Seguridad en bases de datos	Gerencia Técnica Sistemas	1 reporte por gestión acerca de la seguridad de la información	
Sistema de Correspondencia	2. Gestión de activos de información	2.2.3. Protección del archivo	Gerencia General. Sistemas	correos electrónicos de autorización por la MAE o quien designe la misma.	
Restream Encoder transmisiones Presidenciales (youtube)	6. Seguridad de las operaciones	6.1.2. Gestión de cambios	Gerencia Administrativa y Financiera. Contrataciones. Sistemas	2 tarjetas de video SDI	
Servidor NAS de Almacenamiento	6. Seguridad de las operaciones	6.2.1. Respaldos de información	Prensa. Producción. Programación.	Política de uso de almacenamiento para evitar la duplicidad o archivos innecesarios	
	6. Seguridad de las	6.1.2. Gestión de cambios	Sistemas	actualizaciones las más	

	operaciones			recientes a aprobadas											
Ingestas (Almacenamiento masivo de señales audiovisuales) y Testigo 7,1	3. Control de accesos	3.2.1. Administración de accesos, cancelación y privilegios de usuarios	Sistemas. Gerencia Administrativa y Financiera. Contrataciones	1, revisión de usuarios creado correctamente 2, compra de (8) discos duros solidos											
Equipos de Emisión (Play OUT, Servidor Squid, Expresión(Generador de Caracteres))	10. Plan de Contingencias Tecnológicas	10.1.1. Elaboración del plan de contingencias tecnológicas	Gerencia Administrativa y Financiera. Contrataciones. Sistemas	3 discos duros para datacenter											
Hi - Visión	7. Seguridad de las comunicaciones	7.1.1. Gestión de la red	Sistemas	instalación de un punto de red con las mismas característica s del principal											
Router Wi-FI	7. Seguridad de las comunicaciones	7.1.5. Seguridad en redes WiFi	Gerencia Administrativa Financiera. Recursos Humanos. Sistemas	1 capacitación anual al personal que utiliza nuestras redes WI-FI											
Acapella (ROUTER 16X16)	10. Plan de contingencias tecnológicas	10.1.1. Elaboración del plan de contingencias tecnológicas.	Alta Frecuencia	Informes periódicos de los mantenimientos realizados al sistema de respaldo UPS y Grupo Generador.											

VoBo. Elaborado/Actualizado por:	VoBo. Revisado por:

Tablero Eléctrico	10. Plan de contingencias tecnológicas 5. Seguridad física y ambiental	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	Alta Frecuencia	Informes periódicos de los mantenimientos realizados al sistema de respaldo UPS, Grupo Generador y sistema de tierra	
UPS (Sistema de almacenamiento ininterrumpido)	10. Plan de contingencias tecnológicas 5. Seguridad física y ambiental	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	Alta Frecuencia	Informes periódicos de los mantenimientos realizados al sistema de respaldo UPS y Grupo Generador.	
Servicio de Fibra Óptica y equipos de transmisión y recepción.	7. Seguridad de las comunicaciones	7.1.1. Gestión de la red	Alta Frecuencia	Servicio fibra óptica con su respaldo.	
Decoder (HMR)	10. Plan de contingencias tecnológicas 5. Seguridad física y ambiental	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	Alta Frecuencia	Informes periódicos de los mantenimientos realizados al equipo, al sistema de respaldo UPS y Grupo Generador.	

Equipos de monitoreo y medida: monitor forma de onda, vectoroscopio, monitor de audio y analizador de espectro.	10. Plan de contingencias tecnológicas 5. Seguridad física y ambiental	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	Alta Frecuencia	Informes periódicos de los mantenimientos realizados al sistema de respaldo UPS y Grupo Generador.	
Multiplexor	10. Plan de contingencias tecnológicas 5. Seguridad física y ambiental	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	Alta Frecuencia	Informes periódicos de los mantenimientos realizados al equipo.	
Modulador Satelital	10. Plan de contingencias tecnológicas 5. Seguridad física y ambiental	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	Alta Frecuencia	Informes periódicos de los mantenimientos realizados al equipo.	
Uplink (Antena Satelital)	5. Seguridad física y ambiental	5.2.1. Seguridad del Equipamiento	Alta Frecuencia	Informes ocasionales ante el cambio climatológico.	

VoBo. Elaborado/Actualizado por:

VoBo. Revisado por:

| | | |

		equipamiento			
HPA UP LINK (SATELITAL)	10. Plan de contingencias tecnológicas 5. Seguridad física y ambiental	10.1.1. Elaboración del plan de contingencias tecnológicas. 5.2.1. Seguridad del equipamiento	Alta Frecuencia	Informes periódicos de los mantenimientos realizados.	
Cámaras de video broadcast (de Estudio)	1. Seguridad en recursos humanos	1.2.1 Capacitación y formación	Baja Frecuencia	Capacitación realizada	
Cámaras de video broadcast móviles con acceso a Streaming	1. Seguridad en recursos humanos	1.2.1 Capacitación y formación	Baja Frecuencia	Capacitación realizada	
Mesa de Video (Procesador)	1. Seguridad en recursos humanos	1.2.1 Capacitación y formación 6.2.1 Seguridad de las operaciones	Baja Frecuencia	Capacitación realizada. Mantenimiento realizado.	
Mesa de Audio	1. Seguridad en recursos humanos	1.2.1 Capacitación y formación	Baja Frecuencia	Capacitación realizada. Mantenimiento realizado.	
Sistema de intercomunicación	1. Seguridad en recursos humanos	1.2.1 Capacitación y formación	Baja Frecuencia	Capacitación realizada	

CCU (unidad de control central)	5. Seguridad física y ambiental	5.3.1. Condiciones operativas	Baja Frecuencia	Informes de mantenimientos.	
Router Final FOR-A audio/video	10. Plan de contingencias tecnológicas 6. Seguridad de las operaciones.	10.1.1. Elaboración del plan de contingencias tecnológicas 6.2.1 Seguridad de las operaciones	Baja Frecuencia	Informes periódicos de los mantenimientos realizados al sistema de respaldo.	
Fibra Óptica (Dataland)	7. Seguridad de las comunicaciones	7.1.1. Gestión de la red	Baja Frecuencia	Servicio fibra óptica con su respaldo.	
Router Ross Xtreme audio/video	10. Plan de contingencias tecnológicas 6. Seguridad de las operaciones.	10.1.1. Elaboración del plan de contingencias tecnológicas 6.2.1 Seguridad de las operaciones	Baja Frecuencia	Informes periódicos de los mantenimientos realizados al sistema de respaldo.	
Switcher Sony audio/video VCR 7,1	10. Plan de contingencias tecnológicas 6. Seguridad de las operaciones.	10.1.1. Elaboración del plan de contingencias tecnológicas 6. Seguridad de las operaciones	Baja Frecuencia	Informes periódicos de los mantenimientos realizados al sistema de respaldo.	

Master Control audio/video VCR 7,2	10. Plan de contingencias tecnológicas 6. Seguridad de las operaciones.	10.1.1. Elaboración del plan de contingencias tecnológicas 6.2.1 Seguridad de las operaciones	Baja Frecuencia	Informes periódicos de los mantenimientos realizados al sistema de respaldo.												
Sistema de monitoreo de video	5. Seguridad física y ambiental	5.2.1. Seguridad del equipamiento	Baja Frecuencia	Informes de mantenimiento.												
Sistema de monitoreo de audio	5. Seguridad física y ambiental	5.2.1. Seguridad del equipamiento	Baja Frecuencia	Informes de mantenimiento.												
Sistema de refrigeración	5. Seguridad física y ambiental	5.3.1. Condiciones operativas	Baja Frecuencia	Informes de mantenimiento.												