ACTA N° 1
COMITÉ DE SEGURIDAD DE LA INFORMACION.
RESOLUCION RAI/AEMP/DJ/N°42/2020
REF: APROBACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION
Fecha: La Paz, 2 de agosto de 2021.

En fecha 2 de agosto de 2021, a hrs. 11:30, se reúne el COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, designado mediante Resolución Administrativa Interna RAI/AEMP/DJ/N°42/2020 de 17 de diciembre de 2020, para la REVISION DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION – PISI, de acuerdo a las funciones del COMITÉ, previstas en la citada Resolución Administrativa Interna.

Por lo señalado se procedió a la revisión del PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION – PISI que ha sido desarrollado por el Encargado de Sistemas de la entidad, de acuerdo a los *"Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector Público"*, documento 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), como se desprende del Informe AEMP/DAF/CGD/N°344/2021.

El objetivo del PISI es resguardar la información de la institución, en cumplimiento de la normativa referente a la Seguridad de la Información, vigente en el Estado Plurinacional de Bolivia, en ese marco y concluida la revisión y no existiendo observaciones por parte de los miembros del COMITÉ DE SEGURIDAD DE LA INFORMACION, se recomienda al Director Ejecutivo de la Autoridad de Fiscalización de Empresas, efectuar su aprobación mediante Resolución Administrativa.

Abog. Tatiana Gonzales G.
Directora Jurídica -Presidente CSI
Tatiana Esther Gonzales Gandarillas
DIRECTORA JURÍDICA a.i.
Autoridad de Fiscalización de Empresas

Ing. Ronald Cecilio Arraya Veliz
Director de Administración y Finanzas
miembro CSI
Ronald Cecilio Arraya Veliz
DIRECTOR DE ADMINISTRACIÓN Y FINANZAS
Autoridad de Fiscalización de Empresas

Abog. Ramiro Santos Fernández Muñecas
Director Técnico DTFVCOC- miembro CSI
DIRECTOR TÉCNICO DE FISCALIZACIÓN
Y VERIFICACIÓN DE CUMPLIMIENTO
DE OBLIGACIONES COMERCIALES a.i.
Autoridad de Fiscalización de Empresas

Diego Choquehuanca Gutierrez
Encargado de Sistemas- miembro CSI
Diego Choquehuanca Gutiérrez
ENCARGADO DE SISTEMAS
Autoridad de Fiscalización de Empresas

HECHO EN BOLIVIA

RESOLUCIÓN ADMINISTRATIVA INTERNA RAI/AEMP/DJ/Nº 22/2021
La Paz, 3 de agosto de 2021

VISTOS:

La Resolución Administrativa Interna RAI/AEMP/DJ/Nº 042/2020 de 17 de diciembre de 2020, el Informe AEMP/DAF/CGD/Nº344/2021 de 26 de julio de 2021, emitido por el Encargado de Sistemas de la Dirección de Administración y Finanzas, y demás antecedentes:

CONSIDERANDO:

Que mediante Decreto Supremo N°071 de 09 de abril de 2009, se crea la Autoridad de Fiscalización y Control Social de Empresas, que asume las atribuciones, competencias, derechos y obligaciones de la extinta Superintendencia de Empresas, con la función de controlar, supervisar y regular las actividades empresariales, en lo relativo al Gobierno Corporativo, Defensa de la Competencia, Reestructuración de Empresas y el Registro de Comercio.

Que el artículo 46 inciso e) del citado Decreto Supremo, señala que el Director Ejecutivo de la Autoridad de Fiscalización y Control Social de Empresas, tiene la atribución de ordenar o realizar los actos necesarios para garantizar el cumplimiento de los fines relativos de la AEMP.

Que la Ley N° 685 de 11 de mayo de 2015, de Cierre del Proceso de Reestructuración y Liquidación Voluntaria de Empresas y de Atribuciones de la Autoridad de Fiscalización de Empresas, cambia la denominación de la Autoridad de Fiscalización y Control Social de Empresas – AEMP a Autoridad de Fiscalización de Empresas – AEMP, y determina sus competencias y atribuciones.

Que mediante Resolución Suprema No. 27311 de 4 de diciembre de 2020, el Presidente del Estado Plurinacional de Bolivia designó al Lic. German Prudencio Taboada Párraga, Director Ejecutivo de la Autoridad de Fiscalización de Empresas-AEMP.

CONSIDERANDO:

Que la Ley General de Telecomunicaciones, tecnologías de información y comunicación N° 164 de 8 de agosto de 2011, en el parágrafo I del Art. 72 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.

AEMP V°B° Tatiana E. Gonzales G. D.J.

HECHO EN BOLIVIA

Que el Decreto Supremo N°1793 de 13 de noviembre de 2013 (Reglamento a la Ley N° 164 de 8 de agosto de 2011) en su artículo 8, dispone que las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad.

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

Que conforme dispone el inciso f) del Art. 7 del Decreto Supremo N° 2514 de 9 de septiembre de 2015 el Concejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia –CTIC-EPB mediante Resolución Administrativa AGETIC/RA/0051/2017 de 18 de septiembre de 2017, aprobó los "*Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector Público".*

CONSIDERANDO:

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

Que mediante Resolución Administrativa Interna RAI/AEMP/DJ/N°042/2020 de 17 de diciembre de 2020 designa al Responsable de Seguridad de la Información (RSI) de la Autoridad de Fiscalización de Empresas y dispone la conformación del Comité de Seguridad de la Información de la Autoridad de Fiscalización de Empresas.

Que del Informe AEMP/DAF/CGD/N°344/2021 de 26 de julio de 2021 del Encargado de Seguridad de la Información, se establece que se ha desarrollado el **Plan Institucional de Seguridad de la Información – PISI de la Autoridad de Fiscalización de Empresas**, de acuerdo a los *"Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector Público",* documento 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.

Que conforme al ACTA N° 1 del COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, designado mediante Resolución Administrativa Interna RAI/AEMP/DJ/N°42/2020 de 17 de diciembre de 2020 y de acuerdo a las funciones asignadas, procedió a la revisión del PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION – PISI no existiendo

observaciones, recomendando al Director Ejecutivo de la Autoridad de Fiscalización de Empresas, efectuar su aprobación mediante Resolución Administrativa.

Que el objetivo del PISI es resguardar la información de la institución, en cumplimiento de la normativa referente a la Seguridad de la Información, vigente en el Estado Plurinacional de Bolivia y citada en la presente Resolución.

POR TANTO:

EL DIRECTOR EJECUTIVO DE LA AUTORIDAD DE FISCALIZACIÓN DE EMPRESAS (AEMP), en ejercicio de las atribuciones conferidas por el ordenamiento jurídico vigente.

RESUELVE:

PRIMERO,- APROBAR el Plan Institucional de Seguridad de la Información – PISI de la Autoridad de Fiscalización de Empresas, que en anexo forma parte indisoluble de la presente Resolución.

SEGUNDO.- INSTRUIR a la Dirección de Administración y Finanzas de la Autoridad de Fiscalización de Empresas la publicación de la presente Resolución, en la página web de la entidad.

Regístrese, comuníquese, cúmplase y archívese.

DJ/TGG

Tatiana Esther Gonzales Condarcitas
DIRECTORA JURÍDICA a.i.
Autoridad de Fiscalización de Empresas

German P. Taboada Parrayu
DIRECTOR EJECUTIVO
Autoridad de Fiscalización de Empresas

ESTADO PLURINACIONAL DE BOLIVIA
AEMP
Autoridad de Fiscalización de Empresas

HECHO EN BOLIVIA

ESTADO PLURINACIONAL DE
BOLIVIA

MINISTERIO DE DESARROLLO
PRODUCTIVO Y ECONOMÍA PLURAL

AUTORIDAD DE FISCALIZACIÓN DE EMPRESAS

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

LA PAZ - BOLIVIA

HECHO EN BOLIVIA

Calle Batallón Colorados N°24 - Edif. El Cóndor Piso 11. La Paz - Bolivia
Telf./Fax: (591-2) 2150000 - 2152118 - 2152119 aemp@autoridadempresas.gob.bo
www.autoridadempresas.gob.bo

Contenido

Calle Batallón Colorados N°24 - Edif. El Cóndor Piso 11. La Paz - Bolivia
Telf./Fax: (591-2) 2150000 - 2152118 - 2152119 aemp@autoridadempresas.gob.bo
www.autoridadempresas.gob.bo

1. Introducción

La Autoridad de Fiscalización de Empresas - AEMP es una entidad pública descentralizada que regula, controla, supervisa que las empresas se desarrollan en un marco de legalidad en lo relativo a la Defensa de la Competencia, Gobierno Corporativo y Registro de Comercio.

En su estructura orgánica se encuentra el área de Sistemas, cuya función es mantener la funcionalidad permanente de los diferentes sistemas de información y servicios informáticos que actualmente tiene esta Autoridad, además de seguir con los lineamientos establecidos por las demás Entidades del Estado Plurinacional, garantizando que las acciones tendientes al funcionamiento de la AEMP, cumpla con la normativa vigente.

Es importante ofrecer un proceso de mejora y estabilidad en estos servicios de los cuales dependerán las aplicaciones disponibles para satisfacer las actividades de la AEMP y el actuar tecnológico que en general apoya todas las labores de esta Autoridad, por lo cual desde el Área de Sistemas, se deben realizar esfuerzos para mantener en una mejora continua esta oferta para proveer a las Direcciones Técnicas de la AEMP, los equipos TIC siempre disponible con las mejores condiciones técnicas posibles para el actuar institucional.

Así mismo, todas estas labores se encaminan hacia garantizar la integridad y confiabilidad absoluta de todos los activos de información disponibles, llevando la utilización e implementación de Sistemas de Información, hacia la eficiencia y eficacia requerida.

Por otra parte, en cumplimiento a la disposición transitoria segunda del Decreto Supremo N°2514 de 19 de septiembre de 2015, se elaboró el presente Plan Institucional de Seguridad de la Información, basado en el documento "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", elaborado por el Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia.

AEMP V°B° Ronald C. Arraya V. DAF

AEMP V°B° Ramiro S. Fernández M. DTFVCOC

2. Marco Normativo

- El parágrafo I del Artículo 72 de la Ley N° 164 de 28 de julio de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación que dispone

HECHO EN BOLIVIA

que: "El Estado en todos sus niveles, fomentará el acceso y 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 y especialmente para aquellos con menores ingresos y con necesidades especiales".

- El inciso d) del Atrículo 4 (Principios), parágrafo II, del Decreto Supremo N° 1793, de 13 de noviembre de 2013, que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, que dispone que: "se debe implementar los controles técnicos y administrativos que se requieran para preservar la fiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudolento".
- El articulo 8 (Plan de contingencia) del Decreto Supremo N° 1793, de 13 de noviembre de 2013, que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, dispone lo siguiente: "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 09 de septiembre de 2015, en los siguientes artículos, incisos o disposiciones transitorias:
    - Inciso f) del Artículo 7, que dispone 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 dispone entre las funciones de la AGETIC, "Elaborar, proponer, promover, gestionar, articular y actualizar el Plan Implementación de Gobierno electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público;

- 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 dispone 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 dispone que "Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII".
- Parágrafo II del Artículo 18, que dispone que "Las entidades del sector público, en el marco de la Soberanía Tecnológica, deben designar un Responsable de Gobierno Electrónico y Tecnología de Información y Comunicación y un Responsable de Seguridad Informática, encargados de coordinar con la AGETIC".

3. Proceso de Elaboración del PISI

3.1. Etapa Inicial

Se identificaron las siguientes fuentes principales de insumo para la elaboración del presente Plan Institucional de Seguridad de la Información:

- Plan Estratégico Institucional
- Manual de Funciones
- Manual de Procesos y Procedimientos

Dadas las características de los trabajos que se realiza en la Autoridad de Fiscalización de Empresas, no se requirió la realización de Evaluación de Riesgos Previos.

3.1.1. Organización Interna

3.1.1.1. Designación del Responsable de Seguridad de la Información (RSI)

El funcionario responsable de Seguridad de la Información de la AEMP, es el Encargado de Sistemas de la Entidad.

3.1.1.2. Conformación del Comité de Seguridad de la Información

El Comité de Seguridad de la Información será compuesto por los siguientes servidores públicos:

- Director de Administración y Finanzas
- Asesor /a General
- Responsable de Planificación
- Responsable de Seguridad de la Información – Encargado de Sistemas

3.2. Etapa de Desarrollo - Estructura y Contenido del Plan Institucional de Seguridad de la Información - PISI

3.2.1. Objetivo

Establecer el Plan Institucional de Seguridad de la Información de la Autoridad de Fiscalización de Empresas, en concordancia con la normativa vigente.

3.2.2. Alcances

Considerando la misión, visión y objetivos estratégicos de la AEMP, se determina el alcance del Plan Institucional de Seguridad de la Información, mismo que contempla la información institucional, que consiste en información generada por los funcionarios, clasificada de la siguiente manera:

- Correspondencia
- Información Administrativa
- Información de los procesos administrativos y coactivos

3.2.3. Metodología de Gestión de Riesgos

- Identificación, clasificación y valoración de activos de información

  En la Autoridad de Fiscalización de Empresas se identificaron tres activos de información, que consiste en:

  - Correspondencia
  - Información Administrativa

- Información de los procesos administrativos y coactivos

La Clasificación de la Información identificada, se encuentra dentro de: Los procesos relevantes para la AEMP, que se encuentra en soporte físico o digital que, de acuerdo al PISI consiste en: Información Estratégica, Información relacionada con el archivo personal, información relacionada a la documentación administrativa, legal, procesos de adjudicación y otros que tengan un costo económico y de cumplimiento con la normativa legal. También se encuentra la información de archivos tales como respaldos, documentos, credenciales de acceso, entre otros.

La valoración de la información identificada, se detalla a continuación:

Correspondencia

Disponibilidad	Alta
Integridad	Muy Alta
Confidencialidad	Medio

Información Administrativa

Disponibilidad	Muy Alta
Integridad	Alta
Confidencialidad	Medio

Información de los Procesos Administrativos y Coactivos

Disponibilidad	Muy Alta
Integridad	Alta
Confidencialidad	Alta

- Evaluación del Riesgo

Correspondencia

Identificación del Riesgo	En cuanto a vulnerabilidades que presenta la Correspondencia, se puede

	mencionar que las mismas se encuentran expuestas a extravíos, debido al descuido o mala manipulación por parte de los funcionarios que en su mayoría trabajan con correspondencia. De igual manera la correspondencia, tiene amenazas como: Fuego (incendios), condiciones inadecuadas de temperatura o humedad, robo, destrucción de correspondencia, y fugas de la misma.
Análisis y Valoración del Riesgo	La situación de la Correspondencia de la AEMP, tiene la presente situación, basado en la ausencia de actas de confidencialidad, en algunos casos o procesos que se lleven adelante, asimismo, y considerando que la correspondencia es impresa y la misma es archivada en el mismo formato, se tiene la siguiente situación actual: Los estantes donde terminará esta información archivada, no son los adecuados, muebles sin seguridad en el acceso como chapas, o llaves.

Información Administrativa

Identificación del Riesgo	En cuanto a las vulnerabilidades que se tiene en cuanto a la información administrativa de la AEMP y

	considerando que se encuentra en formato físico misma que debe ser archivada, se identificaron las siguientes vulnerabilidades: Estantes inadecuados, muebles sin chapa o llave, inexistencia de acta de confidencialidad, para algunos casos.
Análisis y Valoración del Riesgo	La situación de la información administrativa, considerando que la misma se maneja en formato físico, desde su creación hasta su archivo, es la siguiente: no se encuentra en estantes o muebles adecuados y seguros, así también, la inseguridad en las mismas, con chapa o llave, que pueden ocasionar fuga de información o destrucción de la misma, además de encontrarse expuesta a fuego (incendios), robo, destrucción de la información.

AEMP VºBº Diego Chambehuanca DAF

Información de los Procesos Administrativos y Coactivos

Identificación del Riesgo	En cuanto a las vulnerabilidades con la información de los procesos administrativos y coactivos, se identificaron las siguientes, fuga de información, robo o destrucción de la misma, ocasionados por un descuido o mala manipulación de la misma, de igual manera corre el riesgo de sufri

AEMP VºBº Ronald C. Arraya V. DAF

AEMP VºBº Ramiro S. Fernández M. DTFVCOC

V.º B.º Tatiana Gonzales

HECHO EN BOLIVIA

	copias no autorizadas, que incide en la confidencialidad, integridad y disponibilidad de la mencionada documentación.
Análisis y Valoración del Riesgo	Respecto al análisis de riesgo mencionado, se debe aclarar que, el acto administrativo, toda declaración, disposición, o decisión de la Administración Pública, de alcance general o particular, emitida en ejercicio de la potestad administrativa, normada o discrecional, cumpliendo con los requisitos y formalidades establecidos en la Ley 2341, que produce efectos jurídicos sobre el administrado, son documentos legales importantes que determinan plazos a cumplir por el agente regulado o contiene disposiciones de cumplimiento para los servidores públicos de la AEMP y la falta de alguno de estos documentos, evita el desarrollo normal de las atribuciones de la Autoridad de Fiscalización de Empresas.

- *Tratamiento del riesgo*

  Debido a los riesgos mencionados a los que la AEMP se encuentra expuesta, se realizará la siguiente acción para el tratamiento del mismo, con el fin de reducir y evitar el mismo, para esto se realizarán backups, Basado en el Manual de Procesos y Procedimientos de la AEMP, así mismo se realizará el

almacenamiento de una copia digitalizada de la información generada en las Direcciones de la Autoridad, en la Central de Información y un resguardo adicional se encontrará en el backup de la Central de Información, mismo que se realizará mensualmente.

- *Controles Implementados y por Implementar*

  En cuanto a controles para el Tratamiento de Riesgo de la Autoridad de Fiscalización de Empresas, se aplican dos tipos de controles:

  - Niveles de Acceso
  - Registro de Consultas

3.2.4. Política de Seguridad de la Información (PISI)

a) La protección de la información ante amenazas que se originan del Recurso Humano, será realizada mediante la generación de backups de la información que manejan los funcionarios y de los documentos legales, generados en esta Autoridad.

De igual manera se aplicarán políticas de limitación de privilegios de administrador en el equipo de computación asignado a los funcionarios.

b) El uso de los activos de información, así como la protección de estos activos, será controlado mediante la limitación a la información compartida, tal como el acceso en modo lectura a la Central de Información, por parte de todos los funcionarios públicos de la AEMP, esto para proteger los datos que contiene la mencionada central. De igual manera, se realizará el inventario físico y lógico de los equipos de TI, asignados a los funcionarios de la AEMP, para tener un registro base de los activos de información y verificar el mantenimiento de los mismos a través de revisiones sorpresa. Finalmente, los activos de información serán resguardados, mediante la limitación de los usuarios evitando que los mismos tengan privilegios de administrador.

AEMP V°B° Ronald S. Arraya M. DAF

AEMP V°B° Ramiro S. Fernández M. OTFVCOC

HECHO EN BOLIVIA

c) El Control de accesos a recursos de red, información, sistemas y aplicaciones será realizado mediante accesos que se configuren de acuerdo al requerimiento que realicen los funcionarios, debidamente autorizado por el inmediato superior, para poder acceder a recursos compartidos en la red, y los permisos que deseen tener al momento de acceder, así como los permisos y roles que se asignen a un determinado funcionario.

d) La Autoridad de Fiscalización de Empresas, en la mayoría de los casos, no realiza la transmisión de información a través de redes de comunicaciones, la publicación de información se realiza mediante la página web institucional, misma que contiene la protección de la información publicada, codificando la misma, para que solo contenga permisos de impresión y no así de edición.

e) Las áreas donde se genera, procesa, transmite y almacena información considerable sensible y crítica de la Autoridad de Fiscalización de Empresas, se encuentra con cámaras de seguridad, sin embargo, se considerará la implementación de un sistema de acceso a las oficinas e instalaciones consideradas sensibles y críticas.

f) Considerando que en la Autoridad de Fiscalización de Empresas no se desarrolla Sistemas de Información o Software, debido a que cuenta con un funcionario con el cargo de Encargado de Sistemas, mismo que debe administrar y Gestionar Sistemas de Información, Redes de Comunicación, Infraestructura, Soporte Técnico, entre otras actividades, solo se aplicará la seguridad en el ciclo de vida de los sistemas y/o software que se adquiera, haciendo seguimiento a la metodología de desarrollo y realizando pruebas de la funcionalidad de seguridad conforme avance el proyecto.

g) La gestión de incidentes en seguridad de la información y la mitigación temprana de los mismos dará continuidad a las operaciones y procesos que se realizan en la AEMP, tratando en todo momento de evitar el perjuicio con el desempeño laboral de los funcionarios de esta Entidad.

h) La información física documental, actualmente se encuentra en proceso de digitalización, de manera retroactiva, sin embargo, desde la gestión 2018 se

HECHO EN BOLIVIA

instruyó a las Direcciones de esta Autoridad, la digitalización y remisión de la documentación más relevante para adicionar a la Central de Información, Servidor donde se almacena de manera digital, toda la documentación escaneada, y los usuarios tienen acceso solo de lectura a esta información, con lo que la información física documental que ingresa a la AEMP, se encuentra digitalizada y asegurada.

Por otra parte, la información física documental, se encuentra protegida y archivada en un ambiente dentro del edificio donde se encuentran las instalaciones de la Autoridad de Fiscalización de Empresas, este ambiente se encuentra independiente de las oficinas donde se desarrolla el trabajo cotidiano.

3.2.4.1. Estructura de la Política de Seguridad de la Información

- **Introducción**

  La Autoridad de Fiscalización de Empresas - AEMP es una entidad reguladora de actividades empresariales en lo relativo a la Defensa de la Competencia, Gobierno Corporativo y Registro de Comercio.

  La Autoridad de Fiscalización de Empresas - AEMP, en atribución a sus funciones de regular supervisar y controlar que las empresas se desenvuelvan en un marco legal en lo relativo a la Defensa de la Competencia, Gobierno Corporativo y Registro de Comercio, que concluyen en la emisión de una Resolución Administrativa que puede ser sancionatoria o no.

- **Términos y Definiciones**

  Activo de Información. – Conocimientos o datos que tienen valor para la organización

  Seguridad de Información. – La seguridad de la información consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información; además, pueden estar involucrados otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

  Usuario de Información. – Persona autorizada que accede y utiliza la información en medios físicos o digitales para propósitos propios de su labor.

AEMP VºBº Ronald G. Arraya DAF
AEMP VºBº Ramiro S. Fernández M. DTFYCOC
AEMP VºBº Tatiana E. González G.
HECHO EN BOLIVIA

Servidor Público. – Persona individual, que independientemente de su jerarquía y calidad, presta en servicios en relación de dependencia a una entidad, u otras personas que presten servicios en relación de dependencia, cualquiera sea la fuente de su remuneración.

- **Objetivo General**

  Resguardar los activos de información generados en la Autoridad de Fiscalización de Empresas, respecto a la confidencialidad, integridad y disponibilidad de la misma.

- **Objetivos Específicos**
  - Reglamentar la seguridad en la gestión de los activos de información.
  - Desarrollar un reglamento sobre la Gestión de Riesgos de los Activos de Información.
  - Crear un plan de Gestión de incidentes de Seguridad de la Información
  - Gestionar Capacitación para los funcionarios públicos de la AEMP, en cuanto a temas de Seguridad de Activos de Información, para concientizar sobre la sensibilidad que tienen estos activos.
  - Aplicación de Seguridad a todos los documentos que se publican.
- **Alcance**

  A través de la implementación de la Política de Seguridad de la Información, la Autoridad de Fiscalización de Empresas protegerá los Activos de Información existentes y generados por esta Autoridad, de acuerdo al cumplimiento de los mecanismos indicados en los Objetivos Específicos.

- **Roles y Responsabilidades**

  Comité de Seguridad de la Información – CSI. – Gestión, promoción, control e impulso de iniciativas de las políticas de seguridad.

  Responsable de Seguridad de la Información – RSI. – Gestión, planificación desarrollo e implementación de las políticas de seguridad.

Responsables de Activos de Información. – Establece los requisitos de seguridad y clasificación de la información vinculada al activo del cual es responsable.
Servidores Públicos. – Cumple las Políticas de Seguridad de la Información.

- **Desarrollo**

  Ámbito de Seguridad. – Seguridad en Activos de Información
  Descripción. – Se implementarán controles de acceso para la protección de los activos de información de la Autoridad de Fiscalización de Empresas, ante amenazas tanto externas, como internas de la institución.

- **Difusión**

  La Autoridad de Fiscalización de Empresas, difundirá mediante la página web institucional, todos los documentos y reglamentos implementados para la Política de Seguridad de Información.

- **Cumplimiento**

  La Política de Seguridad de Información y la documentación asociada a la misma que genere y regule su operatividad, será de cumplimiento obligatorio, para todos los funcionarios públicos de la Autoridad de Fiscalización de Empresas.

- **Sanciones**

  El incumplimiento a la Política de Seguridad de Información de la AEMP, conlleva a sanciones, de acuerdo a la normativa interna de la Autoridad de Fiscalización de Empresas.

- **Histórico de Cambios**

  Toda la documentación generada a partir de la Política de Seguridad de la Información de la AEMP, contará con el respectivo Control de Cambios,

identificando a los actores que se encuentren vinculados a un determinado cambio realizado en los mencionados documentos, así como los responsables que realizaron, aprobaron y modificaron el documento.

3.2.4.2. Controles mínimos de seguridad de la información

I. 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 del vínculo laboral.

a) Términos y Condiciones de relación laboral

Establecer las responsabilidades en el marco de seguridad de la información del servidor público o cualquiera que tenga un vínculo laboral con la Autoridad de Fiscalización de Empresas

i. Acuerdo de Confidencialidad

1. Objetivo

   Prevenir posibles fugas, divulgación no autorizada, mal uso o resguardo de la información generada por la AEMP.
2. Aplicabilidad

   Servidores públicos de la Autoridad de Fiscalización de Empresas o cualquier persona jurídica o natural que tenga vínculo laboral con la AEMP.
3. Directrices
   - **a.** Elaborar el acuerdo de confidencialidad.
   - **b.** Definir las restricciones y alcances del uso de la información, así como roles y responsabilidades
   - **c.** Coordinar con la Dirección Jurídica de la AEMP, la legalidad del acuerdo de confidencialidad.

d. Garantizar la anuencia del servidor público de la AEMP, o cualquier persona natural o jurídica que tenga un vínculo laboral con la Autoridad de Fiscalización de Empresas con el acuerdo de confidencialidad.

e. Revisar y actualizar el acuerdo de confidencialidad en caso de cambios sustanciales en la clasificación de la información o a requerimiento interno.

f. Respetar los datos de carácter personal, garantiza la privacidad y protección de la información personal identificable.

b) Concientización, educación y formación en seguridad de la información

Se debe generar una cultura de seguridad de la información institucional de la AEMP, que involucre a todos los servidores públicos de la AEMP y a cualquier persona natural o jurídica que tenga vínculo laboral con la Autoridad de Fiscalización de Empresas.

i. Capacitación y formación

1. Objetivo

Capacitar en temas relacionados a seguridad de la información

2. Aplicabilidad

Servidores públicos de la AEMP o cualquier persona natural que tenga un vínculo laboral con la Autoridad de Fiscalización de Empresas.

3. Directrices

a. Realizar eventos de concientización sobre la seguridad de la información, donde además se

muestren roles y responsabilidades de los funcionarios para procedimientos de seguridad.

b. Realizar capacitaciones e inducciones 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 de la AEMP a ser capacitados.

c. Informar sobre las responsabilidades adquiridas por acción u omisión e incumplimiento al Plan Institucional de Seguridad de la Información.

d. Informar sobre los medios y puntos de contacto en temas relacionados a seguridad de la información

e. Evaluar el grado de conocimiento de los servidores públicos de la AEMP, respecto al Plan Institucional de Seguridad de la Información.

c) Sanciones o amonestaciones a consecuencia del incumplimiento del Plan Institucional de Seguridad de la Información – PISI

Implementar mecanismos disuasivos y preventivos para los casos de incumplimiento, por acción u omisión, de los documentos normativos relacionados a seguridad de la información.

1. Objetivo

Sancionar el incumplimiento de la normativa de seguridad de la información institucional vigente

2. Aplicabilidad

Servidores públicos de la AEMP y cualquier persona jurídica o natural que tenga un vínculo laboral con la Autoridad de Fiscalización de Empresas.

3. Directrices

a. Establecer las sanciones al incumplimiento de la normativa de seguridad de la información institucional vigente.
b. Verificar la concordancia de la aplicación de las sanciones a los procesos o procedimientos internos de cada entidad o institución pública.
c. Informar sobre los alcances y consecuencias de las sanciones fruto de infracciones al PISI.

d) Desvinculación de personal o cambio de cargo

Es necesario velar por el resguardo de la información e intereses de la Autoridad de Fiscalización de Empresas al momento de la desvinculación o cambio de cargo de algún servidor público o cualquier persona natural o jurídica que tenga un vínculo laboral.

1. Objetivo

   Preservar la disponibilidad, confidencialidad e integridad de la información al momento de la desvinculación o cambio de cargo de algún servidor público de la Autoridad de Fiscalización de Empresas.

2. Aplicabilidad

   Servidores públicos de la AEMP y cualquier persona natural o jurídica, al término o cambio de cargo de la relación laboral

3. Directrices

   a. Elaborar un proceso y procedimiento de desvinculación del personal que considere mínimamente: la devolución de los activos de información bajo custodia, el retiro de credenciales y cuentas de acceso a servicios y sistemas que permitan precautelar la seguridad de la información.

b. Documentar el proceso de desvinculación y cambio de cargo

c. Controlar las copias no autorizadas de información durante la desvinculación

d. Responsabilidades y deberes que serán vigentes aun después de la finalización de la relación contractual.

II. 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.

a) Identificación y responsables de los activos de información

Identificar los activos de información de la Autoridad de Fiscalización de Empresas y definir la responsabilidad para una protección apropiada.

i. Inventario de activos de información

1. Objetivo

Inventariar todos los activos de información dentro de los alcances del Plan de Seguridad Institucional de Seguridad de la Información.

2. Aplicabilidad

Activos de información de la Autoridad de Fiscalización de Empresas

3. Directrices

a. Identificar los activos de información considerando mínimamente: el tipo de activo, el formato, la ubicación, la información de soporte, la información sobre licencias y el valor para la AEMP.

b. Clasificar los activos de información.

c. Asignar un valor cuantitativo y/o cualitativo a cada uno de los activos.
d. Revisar y actualizar el inventario de activos de información mínimamente una vez al año y/o cuando se requiera.
e. Restringir el acceso al inventario solo al personal autorizado de la AEMP.
f. El inventario podrá incluir, en caso de no ser tangible el ciclo de vida de la información donde se considere la creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.

ii. Responsabilidad y custodia de los activos de información

1. Objetivo

   Asignar para cada activo de información un responsable y/o custodio de acuerdo a sus funciones y competencias
2. Aplicabilidad

   Responsables / custodios de los activos de información.
3. Directrices
   a. Identificar a los responsables y/o custodios de activos de información.
   b. Documentar el proceso de asignación y devolución de los activos de información a propietarios y/o custodios.
   c. El responsable identificado en caso de no ser una persona, puede ser una entidad que cuente con las responsabilidades de la dirección aprobada para controlar todo o parte del ciclo de vida de la información, también el propietario puede no tener

AEMP V°B° Ronald C. Arraya DAF
AEMP V°B° Ramiro S. Fernández M. DTFVCOC
AEMP V°B° Tatiana G. González D. F.
HECHO EN BOLIVIA

los derechos de propiedad del activo, pero sí de custodia.

iii. Uso aceptable de los activos de información

1. Objetivo

   Establecer las restricciones y condiciones de uso adecuado de activos de información

2. Aplicabilidad

   Responsables y/o custodios de activos de información

3. Directrices

   a. Definir los requisitos de seguridad en relación a los activos de información

   b. Establecer reglas para el uso correcto de los activos de información dentro y fuera de las instalaciones de la AEMP.

   c. Elaborar e implementar un reglamento de uso aceptable de activos de información, considerando mínimamente los puntos anteriores.

   d. Garantizar la aceptación de las restricciones y condiciones de uso de los activos de información a todos los servidores públicos de la AEMP y cualquier persona natural o jurídica que tenga un vínculo contractual con esta Autoridad, a los cuales se les haya asignado uno de ellos.

iv. Devolución de los activos de información

1. Objetivo

   Precautelar la disponibilidad, integridad y confidencialidad de los activos de información al momento de la desvinculación o cambio de cargo

2. Aplicabilidad

   En casos de desvinculación o cambios de cargos

3. Directrices

   a. Desarrollar e implementar un procedimiento de devolución de activos de información

   b. En los casos donde el funcionario público de la AEMP o un usuario externo cuente con conocimiento importante para las operaciones de continuidad de esta Autoridad, dicha información se debería documentar y trasferir.

b) Clasificación de la Información

Identificar y clasificar la información según el grado de sensibilidad y criticidad para su uso y tratamiento adecuado.

i. Clasificación

1. Objetivo

   Identificar y clasificar la información en relación a su valor, requisitos legales, sensibilidad, criticidad para su uso y tratamiento adecuado en la entidad o institución pública.

2. Aplicabilidad

   Información, en cualquier medio en el que se encuentre.

3. Directrices

   a. Elaborar un procedimiento de clasificación de la información institucional, que contenga los requisitos, nivel de clasificación, los responsables, las restricciones y la gestión de la información en general.

   b. Establecer requisitos de protección para cada nivel de clasificación definido que deberán considerar las

necesidades de la entidad o institución pública respecto a la apertura o restricción de la información.

c. Reclasificación de la información de acuerdo a requerimiento y/o normativa vigente.

ii. Etiquetado y manejo

1. Objetivo

   Manejar adecuadamente la información, acorde a los requisitos y nivel de clasificación establecidos.

2. Aplicabilidad

   Información, en cualquier medio en el que se encuentre.

3. Directrices

   a. Definir dentro del procedimiento de clasificación institucional el proceso de etiquetado de la información en formatos físicos y digitales.

   b. Adecuación del proceso de etiquetado a los niveles de sensibilidad y criticidad establecidos.

   c. Definir los procedimientos de manejo, procesamiento, almacenamiento, transmisión, desclasificación y destrucción segura de la información para cada nivel de clasificación.

iii. Protección del archivo

1. Objetivo

   Gestionar la seguridad del archivo de documentos

2. Aplicabilidad

   Documentación archivada

3. Directrices

   a. Definir un proceso y/o procedimiento para el archivo de documentación institucional

b. Elaborar controles para evitar la modificación y el acceso no autorizado a la información archivada.

c. Elaborar controles para el acceso al archivo

d. Elaborar procedimientos de solicitud de documentación archivada.

e. Elaborar controles para la trazabilidad de la documentación archivada, que permita revisar las modificaciones realizadas.

iv. Eliminación segura de información

1. Objetivo

Eliminar la información de manera segura independientemente del medio en el que se encuentre, de acuerdo a los niveles de clasificación definidos por la entidad o institución pública.

2. Aplicabilidad

Información, en cualquier medio en el que se encuentre.

3. Directrices

a. Establecer y elaborar procesos/procedimientos para la eliminación de información, independientemente del medio en el que se encuentre de acuerdo a los niveles de clasificación definidos por la Autoridad de Fiscalización de Empresas y normativa legal vigente en el Estado Plurinacional de Bolivia.

b. Para la eliminación de información, considerar la normativa legal vigente relacionada a la retención y resguardo de información.

v. Traslado físico de los medios de almacenamiento

1. Objetivo

Proteger los medios de almacenamiento que contienen información contra el acceso, uso y manipulación no autorizada al interior y fuera de las instalaciones de la Autoridad de Fiscalización de Empresas.

2. Aplicación

   Medios de almacenamiento

3. Directrices

   a. Elaborar procesos/procedimientos para el traslado de medios de almacenamiento.

   b. Establecer controles de protección física en medios de almacenamiento que eviten la intercepción, copia, modificación y destrucción.

   c. Mantener un registro de los medios de almacenamiento que permita identificar el contenido y custodio.

   d. En caso de considerar como no necesaria la información almacenada en cualquier medio removible, la misma será retirada de la entidad o institución pública sin posibilidad de recuperación.

III. Control de accesos

Gestionar los accesos a servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario.

a) Documentos normativos y operativos para el control de accesos

Establecer e implementar el reglamento para el control de accesos.

i. Normativa de control de accesos

1. Objetivo

Prevenir el acceso no autorizado a servicios, sistemas y aplicaciones

2. Aplicabilidad

   Aplica a sistemas, servicios y aplicativos de los que hace uso la entidad o institución pública para el cumplimiento de sus funciones

3. Directrices
   - **a.** Elaborar un reglamento de control de accesos
   - **b.** El reglamento deberá establecer el objetivo, alcance, roles, frecuencias y responsabilidades para el control de accesos.
   - **c.** El reglamento deberá ser revisado y actualizado cada cierto periodo de tiempo según normativa interna de la entidad o a la ocurrencia de un cambio significativo.
   - **d.** Establecer sanciones al incumplimiento e infracciones en el control de accesos.
   - **e.** Implementar registros de accesos acorde a las necesidades de la entidad o institución pública.
   - **f.** Se deberá establecer la periodicidad de cambios de información de autenticación.
   - **g.** Establecer en las reglas la premisa" Generar todo está prohibido a menos que se permita de forma expresa".

b) Administración de accesos

Administrar la creación, registro y cancelación de cuentas de acceso para usuarios y las responsabilidades de uso adecuado de la información de autenticación, de parte de los usuarios.

i. **Administración de accesos, cancelación y privilegios de usuarios**

1. Objetivo

   Gestionar la creación y cancelación de cuentas de usuario para los distintos servicios, sistemas y aplicaciones que dispone la Autoridad de Fiscalización de Empresas.

2. Aplicabilidad

   Accesos a servicios, sistemas y aplicaciones.

3. Directrices

   a. Se deberá establecer los requisitos de autorización para la creación asignación de roles y privilegios de una cuenta.

   b. Se deberán establecer procesos/procedimientos que reflejen el flujo de actividades a seguir, responsables, tiempos, quien autoriza, quien es consultado, quién es informado, quién es responsable de la cuenta de acceso y la forma y medio de entrega de las credenciales. Se deberá tomar en cuenta el criterio de menor privilegio.

   c. Se deberá establecer el flujo de actividades a seguir para la revisión y cancelación de accesos al momento de la desvinculación laboral.

   d. Identificar de forma única el acceso de los usuarios. Para esto se recomienda utilizar servicios de autenticación centralizada.

   e. Elaborar procesos/procedimientos especiales para el acceso a servicios privilegiados como bases de datos, sistemas operativos y aplicaciones de administración.

f. Para accesos privilegiados se deberán implementar medidas de seguridad adicionales que permitan monitorear y verificar las actividades acordes a las funciones establecidas.

g. Las cuentas de acceso temporal o de invitados deberán contar con la autorización correspondiente.

h. Habilitar las cuentas de acceso basado en roles de usuario para el procesamiento, administración, consulta o uso de la información.

i. Establecer el periodo de tiempo para gestionar credenciales de cuentas perdidas, robadas o comprometidas.

j. Implementar técnicas seguras para fortalecer la información de autenticación.

ii. Responsabilidades de los usuarios para la autenticación

1. Objetivo

   Asegurar que la información de autenticación tenga un uso responsable acorde al reglamento de acceso

2. Aplicabilidad

   Usuario que cuente con credenciales de acceso a sistemas, servicios y aplicaciones.

3. Directrices

   a. Capacitar u concientizar sobre las responsabilidades del uso de credenciales de acceso.

   b. Se deberá dejar constancia sobre la aceptación del servicio público para el uso responsable de la información de accesos.

AEMP V°B° Diego Ch... DAF

AEMP V°B° Ronald G. Arraya V. DAF

AEMP V°B° Ramiro S. Fernandez M. DTFVCOC

AEMP V°B° Tatiana ... Gonzales

HECHO EN BOLIVIA

c. Los servidores públicos deben evitar mantener la información de autenticación en lugares visibles o de acceso fácil para los demás.
d. Los usuarios deberán cumplir el cambio de contraseñas de acuerdo a la periodicidad y requisitos de seguridad que se establezca en la normativa de control de accesos.
e. La información de autenticación no deberá compartirse sin previa autorización justificada.
f. La información de autenticación no deberá utilizarse para otros fines ajenos a las funciones asignadas de la entidad o institución pública.
g. El usuario propietario de la cuenta de acceso es responsable del uso de la contraseña.

iii. Revisión, eliminación o ajuste de los derechos de acceso

1. Objetivo

   Revisar, eliminar o ajustar los derechos de accesos a servicios, sistemas y aplicaciones.
2. Aplicabilidad

   Cuentas de acceso.
3. Directrices
   a. Revisar periódicamente los derechos de acceso para identificar accesos no autorizados
   b. Se deberá revisar los accesos privilegiados con más frecuencia y renovar los mismos en intervalos de tiempo razonables.
   c. Mantener un registro de las modificaciones de privilegios.

c) Control de accesos a redes y servicios de red

Gestionar el acceso a las redes de datos de la entidad o institución pública para prevenir accesos no autorizados y riesgos. La entidad debe establecer parámetros mínimos de cifrado para proteger la confidencialidad e integridad de la información.

i. Acceso remoto

1. Objetivo

   Establecer un proceso/procedimiento para la gestión de acceso remoto a servicios, sistemas y aplicaciones.

2. Aplicabilidad

   Solicitudes de acceso remoto

3. Directrices

   a. Establecer requisitos técnicos mínimos para la identificación y autenticación de usuarios para una conexión remota.

   b. Se deberá exigir la autorización por parte del propietario de la información.

   c. La entidad deberá definir la información que puede ser accedida y administrada mediante esta conexión, tomando en cuenta la clasificación de la información.

   d. Monitorear los accesos remotos a servicios, sistemas y aplicaciones.

   e. Implementar controles de acceso a los servicios de red o aplicaciones de acuerdo a requisitos de autorización y privilegios de uso.

   f. Previsión de procedimientos de respaldo de continuidad del negocio en caso de fallas en los accesos remotos.

AEMP VºBº Ronald C. Arraya M. DAF

AEMP VºBº Ramiro S. Fernández M. DTFVCOC

HECHO EN BOLIVIA

ii. Acceso por redes inalámbricas

1. Objetivo

   Gestionar la solicitud de accesos a redes inalámbricas de la institución

2. Aplicabilidad

   Solicitudes de acceso a redes inalámbricas

3. Directrices

   a. Elaborar y establecer un proceso/procedimiento para la gestión de acceso a redes inalámbricas

   b. Establecer requisitos técnicos mínimos para la identificación y autenticación de usuarios.

   c. La entidad deberá definir la información a la que se puede acceder mediante esta conexión.

   d. Monitorear los accesos de la red inalámbrica

IV. Seguridad Física y ambiental

Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica para la entidad o institución pública, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.

a) Áreas e instalaciones seguras

Establecer medidas de seguridad física en áreas e instalaciones denominadas seguras o críticas de la entidad o institución pública.

i. Seguridad física en áreas e instalaciones

1. Objetivo

   Prevenir y controlar el acceso físico no autorizado a instalaciones seguras o críticas de la entidad o institución pública

2. Aplicabilidad

   Áreas e instalaciones denominadas seguras donde se genere, procese, almacene o transmita información considerada sensible y crítica.

3. Directrices

   a. Elaborar un reglamento de control de acceso físico
   b. El reglamento debe considerar la identificación de áreas e instalaciones seguras o críticas, requisitos de seguridad para el ingreso de personal autorizado, condiciones de trabajo y operación.
   c. Identificar las áreas e instalaciones consideradas seguras o críticas.
   d. Elaborar procesos / procedimientos de accesos a las diferentes áreas e instalaciones según las características de seguridad de la información.
   e. El acceso a pareas e instalaciones deberá ser autorizado.
   f. Señalizar las áreas e instalaciones denominadas seguras.
   g. Contar con áreas de recepción para el control y autorización de ingreso a las instalaciones de la AEMP.
   h. Instalar sistemas de monitoreo y vigilancia enmarcados en la normativa legal vigente.
   i. Contar con procesos / procedimientos para la entrega de grabaciones de sistemas de monitoreo y vigilancia de la AEMP.
   j. Se deberá contar con el equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente.

AEMP V°B° Diego Chambilanca DAF
AEMP V°B° Ronald C. Arraya V. DAF
AEMP V°B° Ramiro S. Fernández M. DTFVCOC
AEMP V°B° Tatiana Gonzales D.
HECHO EN BOLIVIA

k. Los ingresos y salidas de visitas deberán se registradas, autorizadas y controladas. Así mismo deberán portar la identificación de visitante en lugar visible.

l. Los servidores públicos deberán portar la identificación correspondiente en un lugar visible.

m. La seguridad física perimetral de la AEMP, deberá inspeccionar y verificar el ingreso de elementos que comprometan la seguridad.

n. Implementar mecanismos de alerta al interior exterior de las instalaciones ante la ocurrencia de eventos de seguridad.

o. Se deberán realizar simulacros de evacuación y respuesta ante amenazas internas, externas, ambientales y/o revueltas sociales.

p. Impedir el acceso a las instalaciones a personas no autorizadas que no tienen relación directa o indirecta con las funciones de la AEMP.

q. Contar con señalética visible, para evacuaciones o contingencias de la institución.

ii. Trabajo en áreas e instalaciones seguras

1. Objetivo

   Gestionar las actividades de trabajo y operación dentro de las áreas e instalaciones acorde a los requisitos de seguridad.

2. Aplicabilidad

   Aplicable a áreas e instalaciones seguras

3. Directrices

a. Se deberá definir las acciones permitidas y no permitidas en las áreas o instalaciones consideradas seguras.

b. En instalaciones con información sensible se deberá evitar el trabajo no supervisado a servidores públicos y terceras personas para evitar posibles incidentes de seguridad.

c. El uso de cámaras de seguridad y otros controles deberán estar sujetos a normativa legal, que autorice el uso de las mismas en instalaciones donde se trabaje.

d. El personal que trabaje en estas áreas deberá estar al tanto de las acciones permitidas y no permitidas y firmar un documento de aceptación de las mismas.

b) Equipamiento

Proteger el equipamiento interno y externo de la Autoridad de Fiscalización de Empresas, para prevenir el robo, daño, pérdida o compromiso de los mismos.

i. Seguridad del equipamiento

1. Objetivo

Prevenir y/o minimizar el impacto sobre el equipamiento ante amenazas peligros ambientales y accesos no autorizados.

2. Aplicabilidad

Equipamiento interno y externo de la entidad o institución pública.

3. Directrices

a. Los servidores públicos de la AEMP, deberán conocer los cuidados de seguridad en el uso del equipamiento.
b. Las instalaciones con información y equipamiento crítico para las operaciones de la entidad deberán ser controladas para evitar el acceso no autorizado y su compromiso.
c. Implementar controles para minimizar el impacto ocasionado por condiciones ambientales, incendios, inundaciones, polvo, vibraciones, interferencias eléctricas y otros.
d. Establecer criterios para restringir el consumo de alimentos en proximidades de áreas e instalaciones seguras.
e. Realizar mantenimientos periódicos y pruebas de funcionalidad por personal calificado al equipamiento de acuerdo a las especificaciones del fabricante.
f. Mantener y documentar los registros de fallas de operación del equipamiento, mantenimientos preventivos y correctivos.
g. Se deberá llevar un inventario de las especificaciones técnicas de los equipos adquiridos.
h. Los equipos, la información y el software no se deberán retirar de las instalaciones sin previa autorización, para ellos se debe establecer responsables y responsabilidades
i. Se deberá respaldar la información que contiene el equipo previo a la destrucción de la misma.

ii. Escritorio y pantalla limpia

1. Objetivo

   Minimizar el riesgo de acceso no autorizado para prevenir la divulgación, uso indebido, robo de información o modificación.

2. Aplicabilidad

   Información considerada sensible y crítica

3. Directrices

   a. La información sensible y crítica en medios de almacenamiento físico deben se resguardados bajo llave y otro mecanismo de control.

   b. Bloquear la pantalla cuando se encuentre sin supervisión.

   c. Finalizar sesiones activas en aplicaciones o servicios de redes cuando no sean utilizadas.

   d. Se deberá controlar los medios de almacenamiento conectados a equipo

   e. En instalaciones de atención al público se deberá mantener el escritorio despejado.

   f. Se deberá mantener un monitoreo continuo para el cumplimiento de escritorio y pantalla limpia.

c) **Seguridad física y ambiental en el centro de procesamiento de datos**

Establecer controles de seguridad físico ambiental para la operación del Centro de Procesamiento de Datos – CPD.

i. **Condiciones operativas**

1. Objetivo

   Garantizar las condiciones operativas del centro de procesamiento de datos.

2. Aplicabilidad

   Centro de procesamiento de datos.

3. Directrices
   - **a.** Establecer procesos / procedimientos formales para la administración del CPD, en cuanto a accesos, mantenimiento de equipos, supervisión de trabajos externos y otros no limitativos a la presente directriz.
   - **b.** La instalación física del CPD deberá contar con medidas de seguridad que eviten el acceso no autorizado, la debida separación de otros ambientes que comprometan la operación normal del CPD.
   - **c.** Implementar medidas de seguridad ambiental para minimizar riesgos de incendio, inundación, polvo, humedad, vibraciones, interferencia de suministro de energía, interferencia de las comunicaciones y radiación electromagnética.
   - **d.** En función de los requisitos de seguridad que se establezcan, se deberá implementar controles de autenticación robustos para el acceso al CPD.
   - **e.** El acceso físico a terceros deberá contar con autorización formal y escrita para trabajos al interior del CPD bajo supervisión.
   - **f.** La disposición del equipamiento al interior del CPD debe estar organizado y distribuido.
   - **g.** Se debe elaborar un mapa de la disposición del equipamiento del CPD.
   - **h.** La condición de operación del equipamiento deberá estar bajo especificaciones del fabricante.
   - **i.** Se debe elaborar un mapa de la disposición del equipamiento del CPD.
   - **j.** Se deberá implementar dispositivos de enfriamiento y extracción de aire.

k. El CPD deberá estar debidamente señalizado e iluminado.

l. Se deberá instalar alarmas de detección de fallas en el suministro eléctrico y condiciones ambientales.

m. Se deberá organizar el cableado al interior del CPD, en lo posible cumplir con un cableado estructurado.

n. El suministro eléctrico al equipamiento del CPD deberá estar regulado y cumplir con las especificaciones técnicas.

o. De acuerdo a requerimientos de disponibilidad, se deberá implementar suministro alterno de energía eléctrica y/o banco de baterías.

p. Se deberá programar mantenimientos periódicos del equipamiento del CPD.

V. Seguridad de las comunicaciones

Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos.

a) Gestión de la seguridad en redes

Garantizar la protección y la disponibilidad de la Información en las redes de datos.

i. Gestión de la red

1. Objetivo

   Gestionar y administrar las redes de datos y la información en tránsito por este medio.

2. Aplicabilidad

   Redes de datos.

3. Directrices

   a. Establecer un reglamento para la gestión de la red.

b. El reglamento debe considerar roles y responsabilidades, procedimientos, requisitos de seguridad, tipos, métodos de autenticación, monitoreo, autorización para acceso acorde al control de accesos y ad- ministración de la infraestructura de red.

c. Considerar la implementación de dispositivos de red redundantes para puntos de fallo único donde la disponibilidad sea un factor crítico.

d. Elaborar procesos/procedimientos para la gestión de la infraestructura de red.

e. Implementar controles para el resguardo de la integridad, confidencialidad, disponibilidad, no repudio y trazabilidad de la información transmitida al interior y exterior de la entidad o institución pública.

f. El cableado de red a nivel de núcleo, distribución y acceso deberá estar identificado, etiquetado y ser operativo.

g. Se deberán elaborar y actualizar periódicamente los diagramas de red y documentar la arquitectura de la red.

h. Establecer las condiciones de uso aceptable de internet, considerando restricciones para la conexión a internet, siguiendo el principio del mínimo privilegio que garantice la calidad de servicio.

i. Restringir el ancho de banda para recursos de alto consumo acorde al puesto laboral.

ii. Seguridad en servicios de red

1. Objetivo
2. Aplicabilidad

   Servicios de red internos y externos.
3. Directrices
   a. Implementar controles de conexión, autenticación y cifrado para los servicios de red.
   b. En función de las necesidades de protección de confidencialidad de la información, considerar la implementación de controles para la comunicación segura en servicios de red.
   c. Se recomienda que servicios de red externos se encuentren en una o varias zonas desmilitarizadas.

iii. Seguridad en la red perimetral

1. Objetivo

   Proteger la infraestructura de red interna ante amenazas que se originan de redes ajenas y/o públicas.
2. Aplicabilidad

   Infraestructura de red.
3. Directrices
   a. Implementar controles de seguridad perimetral que protejan la red ante posibles intrusiones.
   b. De acuerdo a los requisitos de seguridad se deberán implementar y do- cumentar reglas de acceso y salida en los dispositivos de seguridad.
   c. Establecer una o varias zonas desmilitarizadas (DMZ).

AEMP V°B° Unidad de Gobernanza DAF

AEMP V°B° Ronald C. Arteaga V. DAF

AEMP V°B° Ramiro S. Fernández M. OTFVCOC

AEMP V°B° Talleres E Gobernanza

HECHO EN BOLIVIA

d. Se deberán implementar reglas de control de salida y registro según corresponda.

e. Se deberá monitorear regularmente la actividad en las redes de datos.

f. Se deberán implementar protocolos de conexión segura.

g. Se deberán implementar, cuando se vea necesario, parámetros técnicos de encriptación para conexiones seguras y reglas de seguridad.

iv. Segmentación de la red

1. Objetivo

Separar la red en subredes de acuerdo a requerimiento institucional.

2. Aplicabilidad

Red institucional, sistemas, servicios, bases de datos, servidores y grupos de usuarios entre otros.

3. Directrices

a. Segmentar la red para los sistemas, servicios informáticos, bases de da- tos, servidores y grupos de usuarios entre otros.

b. Para un uso más eficiente de las redes de datos se recomienda utilizar redes locales virtuales (VLAN).

c. Las regionales deberán tener un subdominio de red específico.

d. Segmentar las salidas de internet relacionadas con el consumo interno de servicios.

e. Se deberán segmentar el dominio institucional interno (DNS interno) del dominio institucional externo (DNS externo).

f. Se deberá establecer una o varias zonas desmilitarizadas (DMZ) de acuerdo a requerimiento.

v. Seguridad en redes WiFi

1. Objetivos

   Gestionar la seguridad de redes WiFi.

2. Aplicabilidad

   Redes WiFi.

3. Directrices

   a. Comunicar e informar las redes WiFi oficiales y autorizadas para uso.

   b. Concientizar sobre el uso seguro de las redes WiFi, que informe sobre los riesgos de conexión a redes desconocidas y no autorizadas.

   c. Implementar una red virtual local dedicada para redes WiFi diferente a la red cableada.

   d. 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.

   e. Utilizar algoritmos de cifrado robustos en las redes WiFi.

b) Seguridad del servicio de mensajería electrónica

Gestionar de forma eficiente y segura el servicio de mensajería y/o correo electrónico.

i. Mensajería y correo electrónico

1. Objetivo

Asegurar la disponibilidad, integridad y confidencialidad de la información transmitida a través de estos servicios.

2. Aplicabilidad

   Mensajería y correo electrónico institucional.

3. Directrices

   a. Elaborar un reglamento de uso aceptable del correo electrónico institucional.

   b. El reglamento debe establecer reglas de uso del servicio de correo electrónico y mensajería.

   c. El servicio de correo electrónico deberá ser independiente y pertenecer a un dominio institucional, evitando el uso de correos comerciales.

   d. El servicio de correo electrónico deberá implementarse en un servidor independiente.

   e. Utilizar técnicas de autenticación robustas, además de control a las re- des de acceso público.

   f. Las cuentas de usuario deberán ser autenticadas para prevenir y controlar la suplantación de correo electrónico.

   g. Utilizar protocolos y puertos seguros para la configuración del servicio de correo electrónico.

   h. Gestionar regularmente el almacenamiento de correo electrónico basura.

   i. Se deberán establecer la restricción de uso para archivos adjuntos.

   j. Se deberá instalar software anti-spam.

c) Control sobre información transferida

Asegurar la información transferida.

i. Transferencia de información

1. Objetivo

   Preservar la integridad y confidencialidad de la información transferida.

2. Aplicabilidad

   Información institucional transferida.

3. Directrices

   a. Definir los requisitos de seguridad para la transferencia de información de acuerdo a la criticidad y sensibilidad de la misma.

   b. Elaborar procesos/procedimientos orientados a prevenir la interceptación, manipulación, duplicación, repetición, descubrimiento no autoriza- do y destrucción de la información transferida en cualquier medio.

   c. Utilizar técnicas de cifrado para transferencia de información sensible y crítica.

   d. Se deberá firmar un acuerdo de confidencialidad para la transferencia de la información entre partes, de acuerdo a la criticidad y sensibilidad de la misma.

VI. 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.

a) Desarrollo y mantenimiento de sistemas

Establecer requisitos de seguridad para el diseño, desarrollo, pruebas y mantenimiento de sistemas nuevos o existentes.

i. Elaboración de la normativa de desarrollo

1. Objetivo

   Normar el desarrollo y mantenimiento seguro de sistemas.

2. Aplicabilidad

   Desarrollo y mantenimiento de sistemas nuevos y existentes.

3. Directrices

   a. Elaborar un reglamento que considere los requisitos de seguridad, ro- les y responsabilidades para el desarrollo y mantenimiento de sistemas apoyado en procesos/procedimientos.

   b. El reglamento debe ser revisable, actualizable y comunicado a las partes interesadas.

   c. Elaborar procesos/procedimientos para el control de versiones, despliegues, pruebas de seguridad, evaluación de vulnerabilidades, codificación segura, nuevos parches, correcciones y otros no limitativos a la presente directriz.

   d. Realizar procesos de gestión de actualizaciones de sistemas en caso de ser necesario. Todos los cambios deben ser probados, validados, evaluados, documentados y comunicados previamente.

ii. Identificación de requisitos de seguridad

1. Objetivo

   Establecer requisitos de seguridad desde el inicio del desarrollo y durante el ciclo de vida del sistema.

2. Aplicabilidad

   Desarrollo y mantenimiento de sistemas.

3. Directrices

a. Identificar requisitos de seguridad para el desarrollo y mantenimiento de sistemas. Una forma de identificar es consultando los registros de incidentes, el valor de la información que representa para la entidad o institución pública, las vulnerabilidades conocidas y/o requisitos de las partes interesadas.

b. Evaluar la criticidad de la información en términos de confidencialidad, integridad y disponibilidad para dotar de mayores controles de seguridad.

c. Los requisitos de seguridad deberán contemplar requerimientos de infraestructura tecnológica como disponibilidad y redundancia de almacenamiento.

d. Considerar como requisito la identificación de tipos de usuarios, autorización, autenticación, ambientes de desarrollo, pruebas y despliegue a producción.

e. Identificar requisitos criptográficos y firma digital.

f. Las partes interesadas deberían formar parte integral durante el proceso de desarrollo.

g. Las partes interesadas deberán coordinar temas relacionados a seguridad, funcionalidad, usabilidad y otros.

h. Considerar la protección y privacidad de los datos personales recolecta- dos a través de las aplicaciones.

iii. Seguridad en el desarrollo y mantenimiento de sistemas

1. Objetivo

Asegurar el desarrollo y mantenimiento de sistemas para evitar un impacto operacional adverso.

2. Aplicabilidad

Desarrollo y mantenimiento de sistemas.

3. Directrices
   - **a.** Establecer procesos/procedimientos para técnicas de programación segura.
   - **b.** Se deberán separar los ambientes de desarrollo, pruebas y producción.
   - **c.** El proceso de desarrollo deberá contar con la documentación necesaria.
   - **d.** Establecer procedimientos para el control de cambios, uso de repositorios seguros, documentar cambios funcionales y de seguridad a producción.
   - **e.** Los cambios a producción deberán ser autorizados y documentados previa realización de pruebas.
   - **f.** Los usos de librerías de terceros deberían ser evaluadas en relación a la funcionalidad, seguridad, fuentes confiables y referenciados localmente.
   - **g.** Elaborar procesos/procedimientos de actualización de seguridad para librerías, bases de datos y software dependiente.
   - **h.** Establecer procesos/procedimientos para la realización de copias de seguridad, estos deben contemplar el medio de almacenamiento, el ambiente y la frecuencia de las copias.
   - **i.** De acuerdo a los requerimientos institucionales, se deberá considerar implementar medidas de seguridad para el acceso físico/lógico a los recursos de los ambientes de desarrollo, pruebas y producción según corresponda.

j. Se deben validar datos de entrada y salida, porque este tema es parte de las vulnerabilidades conocidas de los sistemas.

k. Los procedimientos de desarrollo de sistemas deben aplicar técnicas de ingeniería segura que brinden orientación sobre las técnicas de autentificación, control, validación de datos, sanitización y eliminación de código de depuración.

iv. Interoperabilidad de sistemas

1. Objetivo

Asegurar la transacción e intercambio de información entre sistemas de in- formación.

2. Aplicabilidad

Sistemas que consumen o proveen información a otros sistemas.

3. Directrices

a. Utilizar técnicas de cifrado para transacción e intercambio de información que preserve la confidencialidad e integridad de la información.

b. La información de autenticación de usuarios deberá ser válida y verificable.

c. Utilizar protocolos de comunicación cifrada.

d. Se deberán establecer términos y condiciones de uso del servicio entre las partes.

e. La protección de la información de los sistemas puede involucrar la transferencia o el acceso de la información desde puntos externos o fronteras. En este caso la institución debe tener conocimiento de

AEMP VºBº Dirlo Chuquisaca DAF
AEMP VºBº Ronald C. Arauz V. DAF
AEMP VºBº Ramiro S. Fernandez M. DTFYCOC
AEMP VºBº Adriana E. Gonzales G. DJ

HECHO EN BOLIVIA

las responsabilidades legales y contractuales para seguridad de la información.

v. Pruebas de seguridad

1. Objetivo

   Evaluar la seguridad de los sistemas.

2. Aplicabilidad

   Desarrollo, mantenimiento y adquisición de sistemas.

3. Directrices

   a. Las pruebas de seguridad deberán especificarse desde el diseño del sistema y realizarse durante el proceso de desarrollo del mismo.

   b. Para las pruebas se deberán tomar como referencias las vulnerabilidades conocidas.

   c. Documentar las pruebas de aceptación para desarrollos internos y externos, de acuerdo a los requisitos de seguridad establecidos.

   d. Las pruebas deberán permitir evaluar el cumplimiento de la normativa de desarrollo en cuanto a buenas prácticas de codificación e identificar código malicioso.

   e. Las pruebas se deberán realizar utilizando herramientas como analiza- dores de código, escáneres de vulnerabilidades y otros.

   f. El ambiente de pruebas deberá estar configurado con las mismas características de seguridad que el ambiente de producción.

   g. Las pruebas deben considerar canales ocultos para prevenir accesos no autorizados, monitoreo, validación, denegación de servicios, suplantación.

vi. Seguridad en bases de datos

1. Objetivo

   Gestionar y documentar la seguridad en bases de datos

2. Aplicabilidad

   Bases de datos

3. Directrices

   a. Aplicar recomendaciones de configuración en seguridad provistas por el desarrollador del gestor de base de datos.

   b. Considerar implementar redundancia y alta disponibilidad según requisitos de seguridad establecidos.

   c. Para la gestión de copias de respaldo, se deberán elaborar procesos / procedimientos que establezcan responsables, periodicidad y otros que se considere necesario.

   d. Gestionar usuarios y privilegios para acceso a bases de datos, tablas, funciones y otros.

   e. Las cuentas de usuario deberán tener propietarios con responsabilidades de uso.

   f. Para el acceso de cuentas de usuarios a las bases de datos en ambientes de desarrollo, pruebas y producción, se deberán implementar con- troles de autenticación y autorización.

   g. Las extracciones de datos de producción para las pruebas de funcionalidad deberán considerar la confidencialidad de la misma y los controles necesarios para resguardarla.

   h. Se deberán optimizar las consultas lógicas a bases de datos.

AEMP V°B° Ronald C. Arraya V. DAF

AEMP V°B° Ramiro S. Fernández M. DTFVCOC

HECHO EN BOLIVIA

i. Restringir el uso de cuentas de usuario por defecto.
j. En caso de cambios y/o modificaciones a las bases de datos se deberán realizar pruebas de aceptación y funcionalidad bajo autorización documentada.

b) Seguridad para la adquisición de sistemas

Establecer requisitos de seguridad para la adquisición de sistemas, software y aplicaciones a terceros.

i. Requisitos de seguridad

1. Objetivo

   Contemplar requisitos de seguridad para la adquisición de sistemas, software y aplicaciones.
2. Aplicabilidad

   Adquisición de software, sistemas y aplicaciones.
3. Directrices
   - **a.** Se deberán establecer los requerimientos de seguridad y aceptación de acuerdo a la normativa de desarrollo institucional en los términos de referencia.
   - **b.** Comunicar la normativa de desarrollo a las partes interesadas en el pro- ceso de adquisición y/o desarrollo terciarizado.
   - **c.** Se deberán establecer acuerdos de nivel servicio (SLA) con la parte interesada.
   - **d.** Debe obtenerse en la medida de lo posible, información oportuna de las vulnerabilidades técnicas de los sistemas, software y aplicaciones a ser adquiridos de terceros, así como la información relevante con respecto a actualizaciones y parches.

VII. 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.

a) Gestión de incidentes de seguridad de la información

Reducir la afectación negativa a la seguridad de la información y/o continuidad de las operaciones de la entidad o institución pública.

i. Gestión de incidentes

1. Objetivo

   Establecer lineamientos roles, responsabilidades y procedimientos en la gestión de incidentes, para una respuesta eficaz ante la ocurrencia de eventos adversos relacionados a la seguridad de la información.

2. Aplicabilidad

   Incidentes en seguridad de la información.

3. Directrices

   a. Se deberá elaborar procesos y/o procedimientos de gestión de incidentes de seguridad de la información, los mismos deben establecer roles, responsabilidades informar, evaluar y responder sobre eventos de seguridad.

   b. El RSI deberá identificar el incidente para registrar el mismo, el tratamiento que se le dio y/o escalamiento.

   c. El RSI deberá evaluar cada evento de seguridad clasificarlo para su reporte.

   d. Los incidentes que no puedan ser solucionados deberán ser escalados al Centro de Gestión de Incidentes Informáticos por el RSI.

e. El documento de reporte de incidentes y vulnerabilidades deberá ser socializado a los servidores públicos para que los mismos conozcan los medios de reporte.

f. Ante la ocurrencia de incidentes se deberá recuperar y restablecer la operatividad normal de activos de información.

g. El RSI deberá ser el punto de contacto al interior de la institución y con Responsables de Seguridad de la Información de entidades públicas.

h. Una vez que haya pasado el incidente, se deberán documentar las actividades de respuesta.

i. Se deberá llevar una bitácora de eventos para el análisis posterior sobre los costos asociados al incidente y sobre los cuales se deben implementar soluciones a corto, mediano y largo plazo para reducir la probabilidad de ocurrencia futura.

j. El RSI deberá nominar al personal de respuesta ante incidentes, con la responsabilidad, la autoridad y la competencia necesaria para administrar un incidente y mantener la seguridad de la información.

k. El RSI deberá establecer, documentar, implementar y mantener los procesos, procedimientos y controles para dar respuesta a incidentes de Seguridad de la Información.

l. En caso de ser necesario la institución debe realizar, acorde al incidente, un proceso para administrar y gestionar la evidencia forense.

m. En un proceso de atención a incidentes, el RSI en caso de requerir evidencia forense, podrá involucrar

a un abogado o la Policía Nacional para el comienzo de acciones legales o asesoría sobre la evidencia.

VIII. 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.

a) Implementación del plan de contingencias tecnológicas

La entidad o institución pública debe contar con un Plan de Contingencias Tecnológicas formalizado, actualizado e implementado; aprobado por el Comité de Seguridad de la Información, asignando responsabilidades para su ejecución a los propietarios de los activos de información.

i. Elaboración del plan de contingencias tecnológicas

1. Objetivo

   Definir las estrategias, acciones, procedimientos y responsabilidades para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la restauración de las mismas, dentro de los límites de tiempo establecidos.

2. Aplicabilidad

   El plan de contingencias está circunscrito a los eventos tecnológicos.

3. Directrices

   a. Para la elaboración del Plan de Contingencias Tecnológicas se debe considerar: el análisis y evaluación de riesgos en seguridad de la información;

AEMP V°B° Diego Chocamanca DAF
AEMP V°B° Ronald C. Arraya V. DAF
AEMP V°B° Ramiro S. Fernández M. DTFVCOC
V°B° Tatiana E. Gonzales G.
HECHO EN BOLIVIA

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.

b. Implementar procesos y/o procedimientos de recuperación y restauración de operaciones críticas para cada evento identificado.

c. Cada documento operativo debe incluir responsabilidades, procedimientos, funciones e identificación del personal que ejecutará el plan.

d. Los responsables de activos de información en coordinación con el Comité de Seguridad de la Información definen los tiempos máximos de restauración.

e. La entidad o institución pública deberá identificar los requisitos institucionales para la disponibilidad de los sistemas de información.

f. Cada Plan de Contingencias Tecnológicas deberá describir el enfoque para la continuidad, así como las condiciones necesarias para activar un plan de escalamiento si fuese necesario

ii. Pruebas y mantenimiento del plan de contingencias tecnológicas

1. Objetivo

   El Plan de Contingencias Tecnológicas debe ser sujeto a revisiones periódicas y ejercicios de entrenamiento para asegurar su actualización.

2. Aplicabilidad

   Aplica al Plan de Contingencias Tecnológicas y a los servidores públicos involucrados en el plan.

3. Directrices

   a. El RSI coordinará de manera periódica la ejecución de las pruebas al Plan de Contingencias Tecnológicas para verificar, revisar y evaluar el mismo.

   b. Producto de las pruebas, el RSI podrá incorporar situaciones no cubiertas al plan.

   c. En caso de que las pruebas no sean exitosas, el RSI deberá gestionar la implementación de acciones correctivas o preventivas y ejecutar nuevamente las pruebas hasta cumplir con el objetivo planteado.

   d. Se debe documentar la realización de las pruebas y la implementación de los planes de acción correctivos o preventivos según correspondan.

   e. El RSI, en coordinación con los involucrados, debe realizar revisiones periódicas al Plan de Contingencias Tecnológicas en función a la gestión de incidentes de seguridad de la información y al tratamiento de riesgos tecnológicos.

AEMP V°B° Diego Chuquimia DAF

AEMP V°B° Ronald C. Arraya V. DAF

AEMP V°B° Rabiro S. Fernández M. DITFVCOC

AEMP V°B° Tatiana E. Cales G.

IX. 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.

a) Revisión de controles

HECHO EN BOLIVIA

Evaluar periódicamente el cumplimiento de la normativa documental del Plan Institucional de Seguridad de la Información, verificando que los mismos se encuentran en operación.

i. Revisión

1. Objetivo

   Validar el cumplimiento de los controles de seguridad implementados.

2. Aplicabilidad

   Plan Institucional de Seguridad de la Información.

3. Directrices

   a. El Responsable de Seguridad de la Información, en coordinación con el Comité de Seguridad de la Información, será el encargado de verificar la correcta implementación, aplicación y cumplimiento, debiendo realizar revisiones y evaluaciones periódicas al Plan Institucional de Seguridad de la Información, en las que tomará en cuenta los siguientes criterios.

   b. Identificar causas del incumpliendo.

   c. Acciones para lograr el cumplimiento.

   d. Implementar acciones correctivas y preventivas para lograr un proceso continuo, iterativo y de mejora continua del PISI.

   e. Revisar el cumplimiento de las acciones correctivas o preventivas.

   f. Los propietarios de procesos, activos de información e información serán los responsables del cumplimiento de las acciones correctivas.

g. El RSI informará al CSI el estado de cumplimiento de los controles de seguridad implementados.

ii. Verificación del cumplimiento técnico

1. Objetivo

   Detectar vulnerabilidades técnicas en la infraestructura tecnológica.

2. Aplicabilidad

   Tecnologías de la Información.

3. Directrices

   a. Realizar evaluaciones de vulnerabilidades técnicas y hacking ético.

   b. Los resultados de la evaluación deben permitir identificar debilidades de seguridad para mitigar los mismos en el corto, mediano y largo plazo.

   c. Solicitar a la AGETIC u otras entidades la realización de evaluaciones de seguridad de la información, infraestructura, sistemas informáticos entre otros, en coordinación con el personal de la entidad pública que lo requiera.

   d. Realizar revisiones de cumplimiento técnico, que también involucra una revisión de los sistemas operacionales críticos y sensibles para ver que estos se hayan implementado de forma correcta.

b) Auditoría al Plan Institucional de Seguridad de la Información

Verificar el cumplimiento del Plan Institucional de Seguridad de la Información.

AEMP V°B° Lic. Cheguevarra DAF
AEMP V°B° Ronald C. Arraya DAF
AEMP V°B° Ramiro S. Fernández M. OTFVCOS
V°B° Tatiana E. Gonzales

HECHO EN BOLIVIA

i. Evaluación de cumplimiento del plan Institucional de seguridad de la información

1. Objetivo

   Evaluar el grado de cumplimiento del Plan Institucional de Seguridad y las métricas determinadas para cada control implementado por la entidad.

2. Aplicabilidad

   Plan Institucional de Seguridad de la Información

3. Directrices

   a. La unidad de auditoría interna será la encargada de la revisión del cumplimiento del Plan de Seguridad Institucional de la Información relacionado con los documentos normativos, operativos y métricas.

   b. En caso de ser necesario la unidad de auditoría interna podrá delegar a un especialista la revisión para identificar debilidades técnicas y operativas en los controles para la mejora continua de los mismos.

   c. La entidad o institución pública podrá presentar a la AGETIC los avances en el desarrollo e implementación del Plan Institucional de Seguridad de la Información.

   d. La entidad o institución pública presentará a la AGETIC el Plan Institucional de Seguridad de la Información, de acuerdo a normativa legal vigente en el Estado Plurinacional de Bolivia.

3.2.4.3. Indicadores y Métricas

El Responsable de la Seguridad de la Información – RSI de la AEMP, establecerá 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.

3.3. Cronograma de Implementación

N°	Actividad	Fecha Inicio	Fecha Fin	Responsable/es
1	Elaboración de acuerdo de Confidencialidad de la Información	12/08/2021	31/08/2021	Dirección Jurídica Encargado de Sistemas Funcionarios Públicos
2	Elaborar procedimiento de identificación y clasificación activos de información institucional, etiquetado, manejo, protección, en formatos físicos y digitales, así como los responsables de la misma y sus custodios. Desarrollar e implementar un procedimiento de devolución de activos de información. Definir un proceso o procedimiento para el archivo de documentación digital institucional. Elaborar procedimientos de usos de medios removibles flash (quién, cómo, cuándo y para qué desea acceder). Proceso o procedimiento para la eliminación de información.	01/09/2021	30/09/2021	Encargado de Sistemas Dirección Jurídica Funcionarios Públicos

3	Elaborar un procedimiento para el control de acceso físico a las instalaciones de la AEMP.	15/09/2021	29/10/2021	Dirección de Administración y Finanzas Dirección Jurídica Funcionarios Públicos
4	Reglamento de control de accesos a servicios, sistemas, aplicaciones, equipos de computación. Elaborar y establecer un proceso o procedimiento para la gestión de acceso a redes inalámbricas	01/10/2021	15/11/2021	Encargado de Sistemas Dirección Jurídica Funcionarios Públicos
5	Elaborar procesos o procedimientos formales para la administración del CPD en cuanto a accesos, mantenimiento de equipos, supervisión de trabajos externos y otros. Elaborar procesos o procedimientos de gestión de incidentes de seguridad de la información.	16/11/2021	21/01/2022	Encargado de sistemas Dirección Jurídica Funcionarios Públicos
6	Elaborar el plan de contingencias Tecnológicas	01/02/2022	31/03/2022	Encargado de Sistemas Dirección Jurídica Funcionarios Públicos
7	Difusión de toda la reglamentación generada del Plan Institucional de Seguridad de la Información.	01/04/2022	29/04/2022	Dirección de Administración y Finanzas Dirección Jurídica Funcionarios Públicos

1.2. Aprobación del PISI

El PISI de la AEMP, será revisado por el CSI que impulsará su aprobación ante la Máxima Ejecutiva de la Autoridad de Fiscalización de Empresas.

El PISI es flexible a actualizaciones periódicas en función de la mejora continua de la información.

2. Lineamientos para la Implementación del PISI

2.1. Aplicación de Controles

La Autoridad de Fiscalización de Empresas aplicará controles inicialmente en la elaboración de los procedimientos base para la implementación del PISI institucional y posteriormente se elaborará un cronograma de control de la aplicación del mencionado Plan Institucional.

2.2. Capacitación e Inducción

A partir de la implementación de los procesos o procedimientos, el área de Recursos Humanos en coordinación con el Responsable de Seguridad de la Información de la Autoridad de Fiscalización de Empresas, planificarán actividades de capacitación aplicables a la totalidad de los servidores públicos (fijos, eventuales y de reciente incorporación) en relación al Plan Institucional de Seguridad de la Información y sus manuales, procesos y/o procedimientos.

2.3. Gestión de Incidentes de la Seguridad de la Información

La Autoridad de Fiscalización de Empresas, elaborará procedimientos para la gestión de incidentes, que establecerá con claridad procesos de planificación y preparación, detección y reporte, valoración y decisión, respuesta y erradicación para la mejora continua ante la ocurrencia de incidentes relacionado a la seguridad de la información.

AEMP VºBº Ronald C. Arraya M. DAF

AEMP VºBº Ramiro S. Fernandez M. DTEVCOS

Tatiana E. Gonzales G.

HECHO EN BOLIVIA

2.4. Revisión y mejora Continua

El Responsable de Seguridad de la Información – RSI de la AEMP, promoverá la realización de revisiones periódicas a los controles implementados dentro del PISI, en relación al cumplimiento y eficacia de los procesos y/o procedimientos de la Política de Seguridad de la Información.

3. Revisión de los Lineamientos

En cumplimiento al D.S. 2514 Artículo 7, inciso i), se realizarán actualizaciones periódicas a los lineamientos para la elaboración e implementación del Plan Institucional de Seguridad de la Información de la Autoridad de Fiscalización de Empresas.

Calle Batallón Colorados N°24 - Edif. El Cóndor Piso 11. La Paz - Bolivia
Telf./Fax: (591-2) 2150000 - 2152118 - 2152119 aemp@autoridadempresas.gob.bo
www.autoridadempresas.gob.bo