EBA

Empresa Boliviana de Alimentos

DOCUMENTO NORMATIVO INTERNO

Tipo	Código	Ver.
Reglamento	SGE/SIC/REG-001	01

Titulo

Seguridad de la Información

	NOMBRE	CARGO	FIRMA
Elaborado:	Vivian T. Herrera Justiniano	JEFE DE DEPARTAMENTO DE NORMAS Y CALIDAD	
Revisado:	Juan Félix Villegas Méndez	RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN	
Revisado:	David Quelali Quispe	RESPONSABLE DE SISTEMAS	
Revisado:	Patricia Córdova Pino	GERENTE DE PLANIFICACIÓN Y DESARROLLO	
Aprobado:	Javier Freire Bustos	GERENTE EJECUTIVO	

RESOLUCIÓN ADMINISTRATIVA EBA/GE/N° 074/2019
15 de noviembre de 2019

APROBACIÓN DEL REGLAMENTO DE SEGURIDAD DE LA INFORMACION DE LA EMPRESA BOLIVIANA DE ALIMENTOS Y DERIVADOS.

VISTOS:

Los Informes de la Gerencia de Planificación del Desarrollo, INF/GPD/UTIC/2019-0209 de 2 de octubre de 2019, Informe INF/GPD/UNC/2019-0041 de 7 de octubre de 2019; Informe Legal INF/GE/AL/2019-0289 de 15 de noviembre 2019, antecedentes y normativa legal vigente.

CONSIDERANDO:

Que, la Constitución Política del Estado en su artículo 103, parágrafo I determina que: *"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"*. Asimismo, el parágrafo II, establece que: *"el Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación"*.

Que, la Ley N° 164 de 8 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación en su artículo 72, parágrafo I 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"*.

Que, el artículo 75 parágrafo I de la citada ley, dispone que: *"El nivel central del Estado promueve la incorporación del Gobierno Electrónico a los procedimientos gubernamentales, a la prestación de sus servicios y a la difusión de información, mediante una estrategia enfocada al servicio de la población"*. El artículo 76 establece que: *"El Estado fijará los mecanismos y condiciones que las Entidades Públicas aplicarán para garantizar el máximo aprovechamiento de las tecnologías de la información y comunicación, que permitan lograr la prestación de servicios eficientes"*; asimismo el Parágrafo I del Artículo 77, señala que: *"Los Órganos Ejecutivo, Legislativo, Judicial y Electoral en todos sus niveles, promoverán y priorizarán la utilización del software libre y estándares abiertos, en el marco de la soberanía y seguridad nacional"*.

Que, el Decreto Supremo N° 29894 de 7 de febrero de 2009, de Organización del Órgano Ejecutivo, en su artículo 22, inciso t) establece que: *"el Ministerio de la Presidencia es el ente rector del Gobierno Electrónico y de Tecnologías de la 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"*.

Que, el Decreto Supremo N° 2793 de 13 de noviembre de 2013, en su artículo 4, inciso d), 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 y los registros, evitando su falsificación, extravió, utilización y acceso no autorizado o fraudulento"*.

Que, el Decreto Supremo N° 2514 de 8 de septiembre de 2015, artículo 7, inciso f), sostiene que la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) establecerá *"los lineamientos técnicos en seguridad de la información para las entidades del sector público"*.

Que, 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.

Que, la Resolución Administrativa AGETIC/RA/0051/2017 de 19 de Septiembre de 2017, aprueba los *"Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público"*

CONSIDERANDO:

Que, mediante Decreto Supremo Nº 3592 de 13 de junio de 2018, se crea la Empresa Boliviana de Alimentos y Derivados (EBA), por la fusión a partir de la disolución sin liquidación de la Empresa Pública Productiva Lácteos de Bolivia–LACTEOSBOL, Empresa Boliviana de Almendra y Derivados–EBA, y la Empresa Pública Productiva Apícola–PROMIEL, iniciando actividades el 1 de septiembre de 2018.

Que, conforme al Artículo 3 del citado Decreto Supremo Nº 3592, EBA tiene personalidad jurídica y patrimonio propio, duración indefinida, autonomía de gestión técnica, financiera, administrativa, legal y comercial, de carácter estratégico cuyo fin es generar excedentes económicos para potenciar el desarrollo económico productivo y financiar la atención de políticas sociales del país. El Artículo 9, inciso b) establece, entre las atribuciones y funciones del Gerente Ejecutivo, la de aprobar la organización, estructura, planes, programas, proyectos, reglamentos y manuales necesarios para el funcionamiento y desarrollo de las actividades de la empresa.

Que mediante Resolución Suprema N° 23874 de 21 de agosto de 2018, se designa al ciudadano Javier Dante Freire Bustos como Gerente Ejecutivo de la Empresa Boliviana de Alimentos y Derivados (EBA).

CONSIDERANDO:

Que, el Informe de la Gerencia de Planificación del Desarrollo, INF/GPD/UTIC/2019-0209 de 2 de octubre de 2019, emitido por el Responsable de Sistemas de la EBA, concluye que el Reglamento elaborado cumple con los criterios de la Unidad de Sistemas, por lo que se manifiesta la conformidad técnica, para los 6 capítulos y sus 21 artículos, recomienda remitir el reglamento a las unidades que correspondan para dar curso a los trámites de aprobación necesarios.

Que, el Informe de la Gerencia de Planificación del Desarrollo, INF/GPD/UNC/2019-0041 de 7 de octubre de 2019, emitido por la Unidad de Normas y Calidad, señala que el Reglamento de Seguridad de la Información tiene por objetivo establecer los requisitos y condiciones del proceso de seguridad de la información de la Empresa Boliviana de Alimentos y Derivados. El reglamento contiene 21 artículos contenidos en 6 capítulos, ajustándose a lo establecido en el Manual del Sistema de Gestión Documental en cuanto al contenido y la forma. Asimismo, concluye el citado Reglamento ha sido elaborado, revisado y validado por las instancias responsables de su implementación y recomienda remitir a la Gerencia Jurídica para que se emita informe legal y resolución administrativa.

Que, la Gerencia Jurídica mediante Informe INF/GE/AL/2019-0289 de 15 de noviembre de 2019, concluye que el Reglamento de Seguridad de la Información cuyo objetivo es el establecer los requisitos y condiciones para la elaboración e implementación del proceso de seguridad de información de la EBA, ha sido elaborado en el marco de los lineamientos para la elaboración e implementación de los Planes Institucionales de Información de las entidades del sector público, redactado 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), aprobado por la Resolución Administrativa AGETIC/RA/0051/2017 de 19 de Septiembre de 2017 y se encuentra debidamente fundamentado técnica y legalmente en su procedencia, no contraviniendo ninguna disposición legal vigente.

POR TANTO:

El Gerente Ejecutivo de la Empresa Boliviana de Alimentos y Derivados - EBA, en uso de sus funciones y atribuciones legalmente conferidas;

RESUELVE:

PRIMERO.- Aprobar el **Reglamento de Seguridad de la Información de la Empresa Boliviana de Alimentos y Derivados - EBA,** en sus 6 Capítulos y 21 artículos, que en Anexo forma parte integrante de la presente Resolución Administrativa.

SEGUNDO.- Instruir a la Gerencia de Planificación y Desarrollo su difusión a todo el personal de la Empresa Boliviana de Alimentos y Derivados (EBA), para su conocimiento y aplicación.

Regístrese, comuníquese y archívese.

Javier D. Freire Bustos
GERENTE EJECUTIVO
EMPRESA BOLIVIANA DE ALIMENTOS Y DERIVADOS - EBA

Jorge Rolfe Cordero Figueroa
GERENTE JURIDICA
Empresa Boliviana de Alimentos y Derivados - EBA

JFB/JRC/dca
H.R. I/2019-02575

REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN

EMPRESA BOLIVIANA DE ALIMENTOS Y DERIVADOS

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1. (OBJETIVO)

Establecer los requisitos y condiciones para la elaboración e implantación del proceso de seguridad de la información de la Empresa Boliviana de Alimentos y Derivados – EBA.

ARTÍCULO 2. (MARCO LEGAL)

a) Ley N°164 de 8 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de la Información y Comunicación;
b) Decreto Supremo N°29894 de 7 de febrero de 2009, de Organización del Órgano Ejecutivo que establece que el Ministerio de la Presidencia se constituye en el órgano rector del Gobierno Electrónico y Tecnologías para la Información y Comunicación;
c) Decreto Supremo N°2514 de 9 de septiembre de 2015 de Creación de la Agencia de Gobierno Electrónico y Tecnologías de la Información y comunicación;
d) Decreto Supremo N°3251 de 12 de julio de 2017 de Aprobación del Plan de Implementación de Gobierno Electrónico;
e) Decreto Supremo N°1793 de 13 de noviembre de 2013 del Reglamento de la Ley N°164;
f) NB/ISO/IEC/27000:2010 de Gestión de Seguridad de la Información, para las definiciones.

ARTÍCULO 3. (ALCANCE Y ÁMBITO DE APLICACIÓN)

I. El presente reglamento alcanza a todos los procesos que generan activos de información y que se requiere aplicar controles de seguridad de acuerdo a su naturaleza, tamaño y complejidad de los mismos.
II. Todos los servidores públicos de la EBA son responsables del resguardo físico y electrónico de los activos de información que administran, los medios que la contienen.

ARTÍCULO 4. (DEFINICIONES)

a) **Activo:** es todo aquello que tiene valor para una entidad;
b) **Activo de Información:** Conocimiento o datos que tienen valor para la organización;
c) **Acuerdo de Confidencialidad:** Documento en el cual el servidor público y/o terceros se comprometen a respetar la confidencialidad de la información y a usarla solo para el fin que se estipule;
d) **Amenaza:** Causa Potencial de un incidente no deseado, puede dar lugar a daños en un sistema o en una organización;
e) **Apetito de riesgo:** Nivel máximo de riesgo que una institución o entidad está dispuesta a aceptar o soportar;
f) **Comité de Seguridad de la Información (CSI):** Equipo de trabajo conformado para gestionar, promover e impulsar iniciativas de seguridad de la información;
g) **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados;
h) **Custodio de Activo de Información:** Servidor público encargado de administrar u hacer efectivo los controles de seguridad definidos por el responsable de activos de la información;
i) **Disponibilidad:** propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran;

j) **Impacto:** Cambio adverso en la operación normal de un proceso de la empresa
k) **Integridad:** Propiedad que salvaguarda la exactitud y completitud de la información;
l) **Política de Seguridad de la Información (PSI):** acciones o directrices que establecen la postura de la empresa en relación a la seguridad de la información, incluidas dentro del Plan Institucional de la Seguridad de la Información;
m) **Plan Institucional de Seguridad de la Información (PISI):** Documento que establece las actividades relativas a la organización y gestión de la seguridad de la información de la empresa;
n) **Responsable de Activo de Información:** Servidor Público de nivel jerárquico que tiene la responsabilidad y atribución de establecer los requisitos de seguridad y la clasificación de información vinculada al activo enmarcado al proceso del cual es responsable;
o) **Responsable de procesos:** Servidor público de nivel jerárquico que tiene la responsabilidad y atribución de establecer las actividades, roles y responsabilidades de los procesos;
p) **Responsable de Seguridad de la Información (RSI):** Servidor público responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información;
q) **Riesgo:** Combinación de la probabilidad de un efecto adverso y su consecuencia;
r) **Seguridad de la Información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información; también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad;
s) **Seguridad Informática:** Es el conjunto de normas, procedimientos y herramientas que se enfocan en la protección de la infraestructura computacional y todo lo relacionado con esta y especialmente con la información contenida y circulante;
t) **Servidor Público:** Persona individual que independientemente de su jerarquía y calidad, presta servicios en relación de dependencia de la EBA, cualquiera que sea su fuente de financiamiento;
u) **Usuario de Información:** Persona autorizada que accede y utiliza la información en medios físico o digitales para propósitos propios de su labor.
v) **Vulnerabilidad:** Debilidad de un activo o control, que puede ser explotada por una amenaza.

ARTÍCULO 5. (RESPONSABILIDADES)

I. **Gerente Ejecutivo**
a) Estar informado sobre el estado de seguridad de la información de la EBA;
b) Designar al Responsable de Seguridad de la Información;
c) Conformar al Comité de Seguridad de la Información;
d) Asegurar que los objetivos y alcances del Plan Institucional de Seguridad de la Información sean compatibles con los objetivos del Plan Estratégico Empresarial;
e) Destinar recursos administrativos, financieros y humanos para la elaboración e implementación del PISI;
f) Aprobar el PISI;
g) Cumplir y hacer cumplir el PISI;
h) Asumir acciones necesarias a favor de la seguridad de la información.

II. **Gerente de Gestión Empresarial**
a) Representar al Gerente ejecutivo ante el comité de Seguridad de la Información cuando sea necesario;
b) Apoyar la elaboración del Plan Institucional del Seguridad de la información;

c) Gestionar acciones de coordinación con las diferentes unidades organizacionales de la empresa para apoyar la elaboración tanto de la Política de seguridad de la Información como el Plan Institucional de Seguridad de la Información.

III. **Jefe del Departamento de Tecnologías de la Información y Comunicación:**
- a) Liderar la elaboración del Plan de Seguridad de la Información
- b) Proponer las medidas pertinentes para garantizar la seguridad de la información;
- c) Monitorear la gestión de contingencias tecnológicas;
- d) Otras que en desarrollo e implementación del Plan Institucional de Seguridad de la Información se requieran.

IV. **Gerencia Jurídica**
- a) Proporcionar apoyo y asistencia legal al proceso de propuesta, diseño, elaboración e implantación tanto de la Política de Seguridad de la Información como de ekl Plan Institucional de Seguridad de la Información.

ARTÍCULO 6. (ELABORACIÓN Y ACTUALIZACIÓN)
La elaboración del reglamento el Jefe del Departamento de Tecnologías de la Información y comunicación es responsabilidad del Jefe del Departamento de Tecnologías de la Información y Comunicación; así como de su actualización de acuerdo a los resultados de su aplicación en la EBA o cuando se emitiera normativa nacional sobre la materia que requiera ajustes al reglamento.

ARTÍCULO 7. (APROBACIÓN)
La aprobación del presente reglamento es responsabilidad del Gerente Ejecutivo de la EBA mediante Resolución Administrativa expresa.

ARTÍCULO 8. (DIFUSIÓN Y CUSTODIA DE LOS DOCUMENTOS)
El Jefe del Departamento de Normas y Calidad es responsable de la difusión del reglamento de Seguridad de la Información mediante medios físicos y digitales

El Departamento de Normas y Calidad como responsable del sistema de gestión documental de la empresa, será custodio de los Documentos Normativos Internos en originales.

CAPÍTULO II

MARCO INSTITUCIONAL

ARTÍCULO 9. (COMITÉ DE SEGURIDAD DE LA INFORMACIÓN)
El Gerente Ejecutivo designará al personal que conformará el Comité de Seguridad de la Información (CSI) mediante resolución administrativa. Para la conformación se tomará en cuenta el tamaño de la estructura organizativa, el volumen y la complejidad de sus procesos.

El CSI estará conformado al menos por:

- a) El Gerente Ejecutivo, en calidad de presidente del CSI;
- b) Gerentes de área;
- c) El/Los responsable(s) de Seguridad de la Información.

ARTÍCULO 10. (FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN)
- a) Revisar el PISI;
- b) Promover la aprobación del PISI a través de la MAE

c) Revisar los Manuales de Procesos y/o Procedimientos de seguridad que se desprendan de la Política de Seguridad de la Información incorporada en el PISI;
d) Proponer estrategias necesarias para la implementación y/o fortalecimiento de controles de seguridad en el marco de la mejora continua;
e) Realizar el seguimiento y control de los indicadores y métricas establecidos y definir las acciones que correspondan al respecto;
f) Promover la concientización y capacitación en seguridad de la información al interior de la empresa;
g) Proponer y promover las acciones necesarias en función a la gravedad de los incidentes de seguridad de la información, con el fin de prevenir incidentes futuros;
h) Otras funciones que resulten necesarias para la seguridad de la información.

ARTÍCULO 11. (RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN)
El Responsable de Seguridad de la Información (RSI) será el o la profesional con perfil y experiencia en gestión de seguridad de la información, de nivel jerárquico y con un equipo bajo su supervisión y será designado por el Gerente Ejecutivo.

Sus funciones son:
a) Gestionar, elaborar e implementar el PISI;
b) Realizar la evaluación de riesgos de seguridad de la información en coordinación con los responsables de activos de información;
c) Proponer la política de seguridad de la información (PSI) que estará incorporada dentro del PISI
d) Gestionar el cumplimiento del PISI;
e) Elaborar manuales de procesos y procedimientos de seguridad específicos que se desprendan de los lineamientos del PISI y promover su difusión dentro de la empresa;
f) Sugerir prácticas de desarrollo de software seguro para generar procesos formales que tengan presentes los controles de seguridad necesarios para la empresa;
g) Coordinar la inducción, capacitación, comunicación del personal, en el marco del PISI;
h) Gestionar y coordinar la atención y respuesta a incidentes de seguridad de la información en la empresa;
i) Coadyuvar en la gestión de contingencias tecnológicas;
j) Proponer estrategias y acciones en mejora de la seguridad de la información;
k) Promover la realización de auditorías al PISI;
l) Gestionar la mejora continua de la seguridad de la información;
m) Sugerir medidas de protección ante posibles ataques informáticos que puedan poner en riesgo las operaciones normales de la empresa;
n) Realizar acciones de informática forense, en caso de ser necesario, para identificar, preservar, analizar y validar los datos que puedan ser relevantes;
o) Monitorear la implementación y uso de mecanismos de seguridad que coadyuven a la reducción de los riesgos identificados;
p) Otras funciones que resulten necesarias para preservar la seguridad de la información.

CAPÍTULO III

POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 12. (CONTENIDO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN)

a) La Política de Seguridad de la Información deberá incluir mínimamente y de forma no limitativa principios y posturas de la empresa respecto a:
b) Protección de la información empresarial ante amenazas que se originan del recurso humano;
c) Uso y protección de activos de información;
d) Control de accesos a recursos de red, información, sistemas y aplicaciones;
e) Protección de información transmitida a través de redes de comunicaciones;
f) Protección de áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible o crítica;
g) Seguridad en el ciclo de vida de los sistemas y/o software que se desarrolle y/o adquiera;
h) Continuidad de las operaciones y procesos mediante la gestión de incidentes en seguridad de la información;
i) Protección de información física documental;
j) Otras acciones fruto de la evaluación de riesgo.

La redacción de la Política de Seguridad de la Información de la empresa deberá ser coherente con las normas y leyes del Estado Plurinacional de Bolivia, dando cumplimiento a Normas Básicas Gubernamentales que definen la jerarquía documental, las características y formato de cada documento referido a políticas.

ARTÍCULO 13. (ESTRUCTURA DE LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN)

La estructura de la política de seguridad de la información deberá contener mínimamente los siguientes puntos:

a) **Introducción:** Describiendo antecedentes del documento y temas relacionados a la seguridad de la información;
b) **Términos y Definiciones:** Desglosar y aclarar terminología, acrónimos y palabras utilizadas en la temática de la seguridad de la información;
c) **Objetivo General:** Se debe enfocar en el resguardo de los activos de información de la empresa en aspectos referidos a la confidencialidad, integridad y disponibilidad de la información asociada;
d) **Objetivos Específicos:** Se pueden identificar aspectos relacionados a la gestión de los activos de la información, gestión de riesgos, gestión de incidentes, capacitación y sensibilización de los documentos que regulan la seguridad;
e) **Alcance:** Se deberá circunscribir a toda la empresa y sus procesos y otros aspectos que pueda definir el Comité de Seguridad de la Información;
f) **Responsabilidades:** Se deberá establecer las responsabilidades de todas aquellas unidades organizacionales de la empresa y de los servidores públicos que participen en las diferentes etapas de la formulación, ejecución y evaluación de la política de la seguridad de la información
g) **Desarrollo:** Se debe explicar la postura de la empresa respecto al PISI, los controles de seguridad contemplados de acuerdo al análisis de riesgo;
h) **Difusión:** Se deberá plantear la postura de la empresa en cuanto a la difusión de la documentación generada a partir de ella, así como los medios y mecanismos de difusión;

l) **Cumplimiento:** Se deberá establecer la obligatoriedad de cumplimiento de la Política de Seguridad de la Información;

j) **Sanciones:** Se deberá establecer de forma clara que el incumplimiento a la Política de Seguridad de la Información generará sanciones establecidas el Reglamento Interno de Personal de la EBA.

ARTÍCULO 14. (CONTROLES DE LA SEGURIDAD DE LA INFORMACIÓN)

A fines de implementar la política de la seguridad de la información, EBA deberá contemplar al menos los siguientes controles de seguridad de la información:

a) **Seguridad en Recursos Humanos:** Se establecerán mecanismos de relación entre EBA y el personal a fin de preservar la información a la que se tiene acceso durante y después del vínculo laboral. Los mecanismos mínimamente son:

i. Acuerdo de Confidencialidad;
ii. Concientización, educación y formación en seguridad de la información;
iii. Sanciones a consecuencia del incumplimiento del PISI
iv. Desvinculación laboral o cambio de cargo

b) **Gestión de activos de información:** Con el fin de preservar la integralidad, disponibilidad y confidencialidad de los activos de información se deberá administrar, controlar y asignar responsabilidades en el uso y protección de estos a través de:

i. Identificación y responsables de los activos de información;
ii. Clasificación de la información
iii. Gestión de medios de almacenamiento removibles

c) **Control de accesos:** (gestionar los accesos a los servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario mediante:

i. Documentos normativos y operativos para el control de accesos;
ii. Administración de accesos
iii. Control de acceso a redes y servicios de red.

d) **Criptografía:** el uso de técnicas criptográficas aporta mayores niveles de seguridad para proteger la confidencialidad, autenticidad e integridad de la información, además de no repudio y autenticación mediante:

i. Controles criptográficos

e) **Seguridad física y ambiental:** Asegurar áreas e instalaciones donde se genere, procese o transmita información considerada sensible y crítica para la entidad con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información mediante:

i. Áreas e instalaciones seguras;
ii. Equipamiento;
iii. Seguridad física y ambiental en el centro de procesamiento de datos;

f) **Seguridad de las operaciones:** Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta mediante:

i. Responsabilidad de las operaciones;
ii. Respaldos.

g) **Seguridad de las comunicaciones:** Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos a través de:

i. Gestión de la seguridad en redes;
ii. Seguridad del servicio de mensajería electrónica;

iii. Control sobre la información transferida.

h) **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 mediante:

i. Desarrollo y mantenimiento de sistemas;

ii. Seguridad para la adquisición de sistemas.

I) **Gestión de incidentes de seguridad de la información:** Establecer mecanismos para la gestión de incidentes de seguridad de la información para dar continuidad a las operaciones y mejorar los controles de seguridad implementados a través de:

i. Gestión de incidentes estableciendo lineamiento, roles, responsabilidades y procedimientos en su gestión para una respuesta eficaz ante la ocurrencia de eventos adversos relacionados a la seguridad de la información.

j) **Plan de Contingencias tecnológicas:** Implementar un plan 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 través de:

i. Implementación del Plan de contingencias Tecnológicas.

k) **Cumplimiento:** Asegurar el cumplimiento operativo del PISI que conlleva la política de seguridad de la información t la documentación resultante de la misma mediante:

i. Revisión de Controles;

ii. Auditoria al PISI

ARTÍCULO 15. (PLAN DE SEGURIDAD DE LA INFORMACIÓN)

La EBA elaborará su Plan Institucional de Seguridad de la Información en el marco de los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, de acuerdo al siguiente detalle:

I. **Etapa Inicial**

El objetivo de esta etapa es la organización interna en la EBA para ello, se deberá cumplir todo lo estipulado en los artículos 9, 10 y 11 del Reglamento de Seguridad de la Información.

II. **Etapa de Desarrollo**

Que tiene el objetivo de definir la estructura y contenido del Plan Institucional de Seguridad de la Información, que al menos deberá contener:

a) Introducción, objetivos y alcance;
b) Metodología de gestión de riesgos;
c) Política de seguridad de la información;
d) Cronograma de implementación del Plan;
e) Aprobación del PISI.

La revisión y aprobación del documento final estará bajo responsabilidad del Comité de Seguridad de la Información y del Gerente Ejecutivo de la EBA.

III. **Etapa de Implementación**

Tiene el objetivo de establecer las actividades para la implementación del PISI y comprende:

a) Aplicación de Controles;
b) Capacitación e inducción;
c) Evaluación y Mejora Continua;
d) Gestión de Incidentes.

ARTÍCULO 16. (ALCANCES DEL PISI)
El Comité para la Seguridad de la Información definirá los alcances del PISI en función de los proyectos, procesos y operaciones que sean considerados prioritarios para cumplir con la misión, visión y objetivos estratégicos de la entidad.

CAPÍTULO IV

GESTIÓN DEL RIESGO

ARTÍCULO 17. (GESTIÓN DEL RIESGO)
El PISI contempla la gestión del riesgo en el ámbito de la seguridad de la información, para ello, EBA adoptará un estándar y/o una metodología de gestión de riesgos dentro de los alcances del PISI, con el objetivo de implementar los controles de seguridad o mejorar los controles ya existentes.

La metodología deberá adoptar los criterios de identificación, clasificación y valoración de los activos de información; la evaluación del riesgo y tratamiento del riesgo y controles implementados y por implementar.

El RSI junto con los responsables de los procesos identificados dentro de los alcances del PISI coordinará el proceso de identificación, clasificación y valoración de los activos de información.

ARTÍCULO 18. (EVALUACIÓN DEL RIESGO)
El RSI, en coordinación con los responsables de los procesos identificados, realizará la identificación, análisis y valoración de los riesgos asociados a los activos de información previamente identificados, clasificados y valorados, para poder identificar las vulnerabilidades de los activos de información y amenazas a las cuales están expuestas, realizando las siguientes tareas:

a) **Identificación del riesgo**: se tomará en cuenta las vulnerabilidades y amenazas que inciden en la confidencialidad, integridad y disponibilidad de la información.
b) **Análisis y valoración del riesgo:** Para el análisis y valoración del riesgo se evaluarán las posibles consecuencias de la materialización de una amenaza producto de las vulnerabilidades presentes en los activos de información.

El RSI presentará los resultados de la evaluación de riesgos al CSI para analizar su priorización y tratamiento posterior.

La priorización puede ser establecida a partir del nivel de riesgo máximo definido previamente.

ARTÍCULO 19. (TRATAMIENTO DEL RIESGO)
Los responsables de los activos de información en coordinación con el CSI deberán tomar las decisiones a cerca de las medidas más apropiadas para el tratamiento del riesgo identificado.

Los controles a implementar deberán ser clasificados por el orden de prioridad establecido en la valoración de riesgos y analizados por el CSI para su aplicación, este proceso de implementación contemplará plazos de cumplimiento, capacitación, métodos de evaluación, responsables, recursos y otros que sean necesarios.

ARTÍCULO 20. (CONTROLES IMPLEMENTADOS Y POR IMPLEMENTAR)
Se elaborará un listado con los controles implementados y por implementar, en el que se enumerarán y entre ellos mínimamente se tomarán en cuenta los controles de seguridad de la información establecidos en el artículo 14.

CAPÍTULO V

INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 21. (INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN)
EBA elaborará procedimientos para la gestión de incidentes, se establecerán 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 relacionados con la seguridad de la información.

El RSI se constituye en el contacto al interior y exterior de la EBA para la gestión de incidentes y reportará la ocurrencia de incidentes al Centro de Gestión de Incidentes Informáticos de acuerdo a la normativa vigente.

CAPÍTULO VI

ROL DE AUDITORÍA INTERNA

ARTÍCULO 22. (AUDITORIA AL PISI)
El Departamento de Auditoría Interna de la EBA deberá evaluar, controlar, dar seguimiento al PISI y los controles de seguridad de la información contemplados en el Política de Seguridad de la Información.

El Departamento de Auditoría Interna será el encargado de la revisión de cumplimiento del PISI referido a documentos operativos, métricas o normas de auditoria de la Contraloría General del Estado.

El auditor podrá definir el enfoque de la auditoría interna de forma no limitativa: enfoque a las seguridades, enfoque a la información, enfoque a la infraestructura tecnológica, enfoque al software de aplicación, enfoque a las comunicaciones y redes.

Como resultado de la auditoria expresará opinión independiente respecto a la confidencialidad, integridad, disponibilidad y confiabilidad de la información; el uso eficaz de los recursos tecnológicos; la efectividad del PISI de control interno asociado a las tecnologías de la información y comunicación.