6 Lineamientos para la elaboración del PISI

Las entidades o instituciones públicas deberán elaborar su Plan Institucional de Seguridad de la Información conforme a los lineamientos establecidos en el presente documento.

El siguiente cuadro describe el proceso de elaboración del PISI en sus dos etapas.

Cuadro 1: Proceso de Elaboración de PISI por Etapas

PROCESO DE ELABORACIÓN DEL PISI			
Etapa	Objetivo	Actividades	Responsables
Inicial	Organización Interna	Designación del Responsable de Seguridad de la Información Conformación del Comité de Seguridad de la Información	Máxima Autoridad Ejecutiva
Desarrollo	Estructura y contenido del Plan Institucional de Seguridad de la Información - PISI	Introducción, objetivos, alcances Metodología de gestión de riesgos Política de Seguridad de la Información Cronograma de implementación	Responsable de Seguridad de la Información
	Aprobación del PISI	Revisión y aprobación del PISI	Comité de Seguridad de la Información Máxima Autoridad Ejecutiva

A continuación, la descripción de las actividades involucradas en cada etapa.

6.1 Etapa inicial

La etapa inicial tiene como objetivo la organización interna en la entidad o institución pública para la elaboración de su PISI y comienza por la designación del Responsable de Seguridad de la Información y la conformación del Comité de Seguridad de la Información en la entidad o institución pública por parte de la Máxima Autoridad Ejecutiva (MAE).

En esta etapa, el Responsable de Seguridad de la Información debe identificar las siguientes fuentes principales de insumo para elaborar el PISI:

- Requisitos legales, estatutarios, normativos y contractuales que la institución y sus dependencias hayan establecido con los proveedores de servicio o terceros asociados a la entidad.
- Conjunto de principios y objetivos, Planes Estratégicos Institucionales, Planes Operativos Anuales, manuales de funciones y cualquier otra fuente documental que sirva para el manejo, procesamiento, almacenamiento, comunicación o resguardo de la información, que apoye a las operaciones de la institución.
- Evaluación de riesgos previos que la institución haya realizado: informes, reportes de incidentes y/o cualquier documento relacionado a amenazas o vulnerabilidades a las que la institución haya sido expuesta.
- Cualquier otra documentación interna o externa que la institución determine como apropiada y necesaria para la elaboración del PISI.

6.1.1 Responsabilidades de la Máxima Autoridad Ejecutiva (MAE) respecto a la seguridad de la información

La Máxima Autoridad Ejecutiva deberá:

a) Estar informada sobre el estado de seguridad de la información de la entidad o institución pública bajo su tutela.

b) Tomar conocimiento de la normativa vigente respecto a seguridad de la información (Decreto Supremo N° 2514 de 9 de septiembre de 2015 y Decreto Supremo N° 1793, de 13 de noviembre de 2013, de reglamentación a la Ley 164).

c) Designar al Responsable de Seguridad de la Información (RSI).

d) Conformar el Comité de Seguridad de la Información (CSI).

e) Asegurar que los objetivos y alcances del Plan Institucional de Seguridad de la Información sean compatibles con los objetivos del Plan Estratégico Institucional.

f) En lo posible, destinar los recursos administrativos, económicos y humanos para la elaboración e implementación del Plan Institucional de Seguridad de la Información.

g) Aprobar el Plan Institucional de Seguridad de la Información de su entidad o institución.

h) Cumplir y hacer cumplir el Plan Institucional de Seguridad de la Información de su entidad o institución.

i) Asumir otras acciones a favor de la seguridad de la información.

6.1.2 Designación y funciones del Responsable de Seguridad de la Información (RSI)

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

Independientemente del tamaño de la entidad, el RSI corresponderá a un cargo de nivel jerárquico y deberá contar con un equipo de apoyo bajo su supervisión y coordinación, que coadyuve en el proceso de elaboración e implementación del PISI.

El RSI tendrá las siguientes funciones:

a) Gestionar, elaborar e implementar el Plan Institucional de Seguridad de la Información (PISI).

b) Realizar la evaluación de riesgos de seguridad de la información en coordinación con los responsables de activos de información.

c) Proponer la Política de Seguridad de la Información (PSI), que estará incorporada dentro del PISI.

d) Gestionar el cumplimiento del PISI.

e) Elaborar manuales de procesos y/o procedimientos de seguridad específicos que se desprendan de los lineamientos del Plan Institucional de Seguridad de la Información y promover su difusión en la entidad o institución pública.

f) Sugerir prácticas de desarrollo de software seguro para generar procesos formales que tengan presentes los controles de seguridad necesarios para la entidad o institución.

g) Coordinar la inducción, capacitación y comunicación del personal, en el marco del PISI.

h) Gestionar y coordinar la atención y respuesta a incidentes de seguridad de la información en su entidad o institución.

i) Coadyuvar en la gestión de contingencias tecnológicas.

j) Proponer estrategias y acciones en mejora de la seguridad de la información.

k) Promover la realización de auditorías al Plan Institucional de Seguridad de la Información.

l) Gestionar la mejora continua de la seguridad de la información.

m) Sugerir medidas de protección ante posibles ataques informáticos que puedan poner en riesgo las operaciones normales de la Institución.

n) Realizar acciones de informática forense, en caso de ser necesario, para identificar, preservar, analizar y validar datos que puedan ser relevantes.

o) Monitorear la implementación y uso de mecanismos de seguridad, que coadyuven a la reducción de los riesgos identificados.

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

6.1.3 Conformación y funciones del Comité de Seguridad de la Información (CSI)

Mediante resolución administrativa, la Máxima Autoridad Ejecutiva designará al personal que conformará el Comité de Seguridad de la Información (CSI), de acuerdo al tamaño de la estructura organizativa de su entidad, volumen y complejidad de sus operaciones.

El CSI estará conformado por:

a) La Máxima Autoridad Ejecutiva en calidad de presidente del CSI, con la posibilidad de delegar sus funciones.

b) Personal de nivel jerárquico, de acuerdo a la estructura organizativa de la entidad o institución pública.

c) El Responsable de Seguridad de la Información (RSI).

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

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

a) Revisar el Plan Institucional de Seguridad de la Información (PISI).

b) Promover la aprobación del PISI a través de la MAE.

c) Revisar los manuales de procesos y/o procedimientos de seguridad que se desprendan de la Política de Seguridad de la Información incorporada en el PISI.

d) Proponer estrategias necesarias para la implementación y/o fortalecimiento de controles de seguridad en el marco de la mejora continua.

e) Realizar el seguimiento y control de los indicadores y métricas establecidos y definir las acciones que correspondan al respecto.

f) Promover la concientización y capacitación en seguridad de la información al interior de la entidad o institución pública.

g) Proponer y promover las acciones necesarias en función a la gravedad de los incidentes de seguridad de la información, con el fin de prevenir incidentes futuros.

h) Otras funciones que resulten necesarias para la seguridad de la información.

6.2 Etapa de desarrollo del PISI

Tiene como objetivo establecer las actividades para la elaboración y aprobación del PISI.

6.2.1 Definición de los alcances del PISI

La entidad o institución pública definirá, dentro de su PISI, los alcances relacionados a proyectos, procesos y operaciones considerados prioritarios para cumplir con la misión, visión y objetivos estratégicos de la entidad.[7]

6.2.2 Adopción de una metodología de gestión de riesgos

El PISI contempla la gestión de riesgos en el ámbito de la seguridad de la información. Para esto, la entidad o institución pública deberá adoptar un estándar y/o metodología de gestión de riesgos dentro de los alcances del PISI, con el objetivo de implementar controles de seguridad o mejorar la eficacia de los controles ya existentes.

La adopción de dicha metodología deberá incorporar los siguientes aspectos:

a) Identificación, clasificación y valoración de activos de información

El RSI, de forma conjunta con los responsables de los procesos identificados dentro de los alcances del Plan Institucional de Seguridad de la Información, coordinará el proceso de identificación, clasificación y valoración de activos de información. Para esta parte, se recomienda usar la guía incluida en el Anexo B.

b) 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 ac-

[7] Existen controles mínimos que deberán ser considerados dentro de los alcances del Plan, que están descritos en el punto 6.2.3.2.

tivos de información previamente identificados, clasificados y valorados. Esto le permitirá a la entidad o institución pública identificar las vulnerabilidades de sus activos de información y amenazas a las cuales están expuestas. Las tareas necesarias para la evaluación de riesgos son las siguientes:

Cuadro 2: Evaluación de Riesgos

Tarea	Descripción
Identificación del riesgo	Para la identificación del riesgo se tomarán en cuenta las vulnerabilidades y amenazas que inciden en la confidencialidad, integridad y disponibilidad de la información.
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. Esta priorización puede ser establecida a partir del nivel de riesgo máximo definido previamente por la entidad o institución pública a través del CSI.

c) Tratamiento del riesgo

Los resposables de los activos de información, en coordinación con el RSI, deberán tomar decisiones acerca 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.

d) Controles implementados y por implementar

La entidad o institución pública elaborará un listado de los controles implementados y por implementar, en el que se enumerarán y, mínimamente, se tomarán en cuenta los controles del punto 6.2.3.2. (Controles mínimos de seguridad de la información) y otros que resulten necesarios fruto de la evaluación de riesgos.

Los controles que no sean implementados deberán contar con un respaldo justificado, documentado y aprobado por el Comité de Seguridad de la Información.

Para los puntos b), c) y d) se recomienda el uso de la guía del Anexo B.

6.2.3 Contenido de la Política de Seguridad de la Información (PSI)

La Política de Seguridad de la Información (PSI) deberá incluir mínimamente y de forma no limitativa principios y posturas institucionales respecto a:

a) Protección de la información institucional ante amenazas que se originan del recurso humano.

b) Uso y protección de activos de información.

c) Control de accesos a recursos de red, información, sistemas y aplicaciones.

d) Protección de información transmitida a través de redes de comunicaciones.

e) Protección de áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica.

f) Seguridad en el ciclo de vida de los sistemas y/o software que se desarrolle y/o adquiera.

g) Continuidad de las operaciones y procesos mediante la gestión de incidentes en seguridad de la información.

h) Protección de información física documental.

i) Otras acciones fruto de la evaluación de riesgos.

La redacción de la Política de Seguridad de la Información de la entidad o institución pública 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 referente a políticas.

6.2.3.1 Estructura de la Política de Seguridad de la Información

La estructura de la Política de Seguridad de la Información deberá contener mínimamente los siguientes puntos:

- **Introducción**

  La introducción deberá describir los antecedentes del documento, el asunto o la materia que se desarrollará en relación a seguridad de la información.

- **Términos y definiciones**

  Se debe desglosar y aclarar la terminología, acrónimos y palabras propias utilizadas para el desarrollo de la Política de Seguridad de la Información.

- **Objetivo general**

  El objetivo general se debe enfocar en el resguardo de los activos de información de la institución respecto a la confidencialidad, integridad y disponibilidad de la información asociada.

- **Objetivos específicos**

  Tienen como base al objetivo general y deben establecer la orientación para su consecución. Dentro de los objetivos se pueden identificar temas relacionados a la gestión de activos de información, gestión de riesgos, gestión de incidentes, capacitación y sensibilización de los documentos que regulan la seguridad.

- **Alcance**

  El alcance define la trascendencia y el ámbito de aplicación de la PSI al interior de la entidad o institución.

  Idealmente, debe estar circunscrito a toda la institución y se recomienda que se defina en conjunto con el Comité de Seguridad de la Información.

- **Roles y responsabilidades**

  En este punto se deben establecer los roles del CSI, del RSI, de los responsables de activos de información y del conjunto de servidores públicos, sobre los cuales se definirán las responsabilidades relacionadas con la organización y gestión de la seguridad de la información.

- **Desarrollo**

  Dentro del desarrollo se debe explicar la postura institucional respecto al Plan Institucional de Seguridad de la Información, los controles mínimos de seguridad contemplados, y otros requerimientos de seguridad de la información de acuerdo a los resultados del análisis de riesgo realizado.

  El contenido deberá incorporar el título del ámbito de seguridad, una breve descripción del mismo y la postura institucional respecto a los lineamientos y reglas generales para desarrollar los controles de seguridad.

  Ejemplo.

  Ámbito de seguridad: Seguridad en recursos humanos

  Descripción: Se implementarán controles para la protección de la información institucional ante amenazas que se originan del recurso humano.

- **Difusión**

  La PSI debe contener y describir la posición institucional en cuanto a la difusión de toda la documentación generada a partir de ella, así como los medios y mecanismos de su difusión.

- **Cumplimiento**

  Este punto debe establecer de forma clara la obligatoriedad del cumplimiento de la PSI y de toda la documentación asociada que genere y regule su operatividad.

- **Sanciones**

  Se debe establecer de forma clara que el incumplimiento a la PSI y todo

lo relacionado a la misma conlleva sanciones, que no deben ser descritas puntualmente, sino simplemente hacer referencia a normativa(s) legal(es) existente(s) para ejercer sanciones.

- **Histórico de cambios**

  Se recomienda que la documentación generada a partir de la PSI cuente con el respectivo control de cambios, que identifique a los responsables de la elaboración, aprobación y modificación de la documentación con fechas específicas por cada operación.

6.2.3.2 Controles mínimos de seguridad de la información

La entidad o institución pública deberá implementar mínimamente los siguientes controles de seguridad de la información, conforme a los principios establecidos en la Política de Seguridad de la Información:

a) Seguridad en recursos humanos (Véase el punto 1 del Anexo A).

b) Gestión de activos de información (Véase el punto 2 del Anexo A).

c) Control de accesos (Véase el punto 3 del Anexo A).

d) Criptografía (Véase el punto 4 del Anexo A).

e) Seguridad física y ambiental (Véase el punto 5 del Anexo A).

f) Seguridad de las operaciones (Véase el punto 6 del Anexo A).

g) Seguridad de las comunicaciones (Véase el punto 7 del Anexo A).

h) Desarrollo, mantenimiento y adquisición de sistemas (Véase el punto 8 del Anexo A).

i) Gestión de incidentes de seguridad de la información (Véase el punto 9 del Anexo A).

j) Plan de contingencias tecnológicas (Véase el punto 10 del Anexo A).

k) Cumplimiento (Véase el punto 11 del Anexo A).

6.2.3.3 Indicadores y métricas

El RSI 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.

En general, un indicador y métrica deberá ser:

a) Específico.

b) Medible cualitativa o cuantitativamente y/o con indicadores y atributos.

c) Alcanzable.

d) Relevante.

e) Repetible en periodos de tiempo.

6.3 Cronograma de implementación

En el marco del Plan Institucional de Seguridad de la Información, la entidad o institución pública deberá elaborar un cronograma de implementación de los controles definidos. Para esto, todos los procesos y/o procedimientos que se desprendan de la Política de Seguridad de la Información deberán estar previamente elaborados para su aplicación. El cronograma de implementación deberá contemplar mínimamente:

a) Fechas.

b) Controles a implementarse.

c) Roles y responsabilidades.

d) Actividades relacionadas a capacitación, seguimiento, revisión y aplicación de controles.

La implementación del Plan Institucional de Seguridad de la Información estará sujeta al cronograma y no debería exceder el plazo de un año desde su aprobación por parte de la entidad o institución pública. De acuerdo al contexto de cada institución y sus recursos, este plazo podrá ser ampliado previa justificación escrita por

la MAE y la documentación de respaldo elaborada por el RSI indicando las causales del retraso.

La disposición transitoria segunda del Decreto Supremo 2514 de 9 de septiembre de 2015, establece que: "las entidades del nivel central del Estado deberán presentar a la AGETIC, en un plazo no mayor a un (1) año desde la aprobación de las políticas de seguridad de la información por la AGETIC, su Plan Institucional de Seguridad de la Información".

6.4 Aprobación del PISI

El PISI deberá ser revisado por el CSI que impulsará su aprobación ante la Máxima Autoridad Ejecutiva de la entidad o institución pública.

El PISI deberá ser flexible a actualizaciones periódicas en función de la mejora continua de la seguridad de la información.

7 Lineamientos para la implementación del PISI

Tiene el objetivo de establecer las actividades para la implementación del PISI. El siguiente cuadro describe el proceso antes mencionado.

Cuadro 3: Proceso de implementación de PISI

PROCESO DE IMPLEMENTACIÓN DEL PISI			
Etapa	Objetivo	Actividades	Responsables
Implementación	Implementar el PISI	Aplicación de controles Capacitación e inducción Evaluación y mejora continua Gestión de incidentes	Responsable de Seguridad de la Información Comité de Seguridad de la Información

7.1 Aplicación de controles

La entidad o institución pública deberá aplicar los controles mínimos contemplados en la etapa de elaboración de acuerdo al cronograma de implementación y aprobación establecido dentro del PISI.

7.2 Capacitación e inducción

La capacitación e inducción al personal es parte integral en la implementación del Plan Institucional de Seguridad de la Información. El Área de Recursos Humanos, en coordinación con el RSI, planificará 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 manuales de procesos y/o procedimientos de seguridad, generados a partir de la Política de Seguridad de la Información.

Para este fin, se deberán establecer mecanismos de formación continua en relación al PISI.

7.3 Gestión de incidentes de seguridad de la información

La entidad o institución pública elaborará procedimientos para la gestión de incidentes, que 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 a la seguridad de la información.

El RSI será la persona de contacto al interior y exterior de la entidad o institución pública para la gestión de incidentes y tendrá la responsabilidad de reportar la ocurrencia de los mismos al CGII de acuerdo a normativa vigente.

Las entidades o instituciones públicas que tengan conformados equipos de respuesta ante incidentes informáticos (CSIRT, CERT o similares) deberán reportar sus incidentes y vulnerabilidades identificadas, así como el tratamiento realizado, al Centro de Gestión de Incidentes Informáticos (CGII), de acuerdo al artículo 17 del Decreto Supremo 2514.

El Anexo C contiene una guía para la gestión de incidentes de seguridad de la información.

7.4 Revisión y mejora continua

El RSI deberá promover la realización de revisiones periódicas a los controles implementados dentro del Plan Institucional de Seguridad de la Información, en relación al cumplimiento y eficacia de procesos y/o procedimientos de la Política de Seguridad de la Información.

Los resultados de la revisión permitirán medir la efectividad y cumplimiento de los controles implementados para que, en función de los mismos, se realice la mejora continua de la seguridad de la información.

8 Auditoría al PISI

La unidad de auditoría interna de la entidad o institución deberá evaluar, controlar y dar seguimiento al Plan Institucional de Seguridad de la Información y los controles de seguridad de la información contemplados en la Política de Seguridad de la Información.

La unidad de auditoría interna será la encargada de la revisión de cumplimiento del Plan Institucional de seguridad de la información referida a documentos operativos, métricas o normas de auditoría 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 auditoría, podrá expresar una 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 la comunicación.

9 Presentación del PISI

La entidad o institución pública presentará a la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación su Plan Institucional de Seguridad de la Información de acuerdo a normativa vigente en el Estado Plurinacional de Bolivia.

Opcionalmente, la entidad o institución pública podrá presentar los avances en la elaboración de su PISI.

10 Revisión de los lineamientos

En cumplimiento al Decreto Supremo 2514 Artículo 7, inciso i), se realizarán actualizaciones periódicas a los lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público.