La Paz, 31 de octubre de 2023
DIRECCIÓN GENERAL EJECUTIVA
SERVICIO NACIONAL TEXTIL - SENATEX
RESOLUCIÓN ADMINISTRATIVA SENATEX/DGE/N° 0075/2023

ASUNTO: APROBACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI) DEL SERVICIO NACIONAL TEXTIL – SENATEX.

VISTOS:

El Informe Técnico INF/SENATEX/UGST N° 0299/2023, de 31 de octubre de 2023, emitido en la Unidad de Gestión de Servicios Técnicos y la Unidad de Administración y Finanzas y el Informe Legal INF/SENATEX/UAJ N° 0177/2023, de 31 de octubre de 2023, emitido por la Unidad de Asuntos Jurídicos, todos dependientes del Servicio Nacional Textil – SENATEX; y demás documentación que convino ver y se tuvo presente.

CONSIDERANDO:

Que, el Parágrafo II del Artículo 103 del Texto Constitucional dispone 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".* El Parágrafo II de este mismo artículo, estipula que: *"El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de la información y comunicación".*

Que, la Ley Nº 650, de 15 de enero de 2015, eleva a rango de Ley la "Agenda Patriótica del Bicentenario 2025", misma que en su Pilar 4 establece: "*Soberanía científica y tecnológica con identidad propia*".

Que, el Artículo 71 de la Ley Nº 164, de 8 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación declara de prioridad nacional la promoción del uso de las tecnologías de información y comunicación para procurar el vivir bien de todas las bolivianas y bolivianos. Asimismo, el Parágrafo I del Artículo 72 de la citada Ley, 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 76 de la Ley Nº 164, determina 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.*"

Que, el parágrafo II del Artículo 77 de la Ley Nº 164, de 8 de agosto de 2011, establece que "*...El Órgano Ejecutivo del nivel central del Estado, elaborará el plan de implementación de software libre y estándares abiertos en coordinación con los demás órganos del Estado y entidades de la administración pública.*"

Que, el Artículo 2 del Decreto Supremo Nº 2514, de 9 de septiembre de 2015, dispone la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, como una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica, y patrimonio propio, bajo tuición del Ministerio de la Presidencia.

Que, el parágrafo I del Artículo 8 del Decreto Supremo Nº 2514, crea el Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC, estableciendo dentro de sus funciones el de: "*c) Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público;* (...) *k) Realizar el seguimiento al desarrollo e implementación de los planes de seguridad de la información en las entidades y empresas públicas del nivel central del Estado; (...) y n) Realizar otras tareas orientadas a la mejora de la seguridad de la información de las entidades del sector Público.*"

Que, el Parágrafo III del Artículo 17 del precitado Decreto Supremo, señala que: *"Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el Centro de Gestión de Incidentes Informáticos — CGII."*

Que, el Parágrafo II del Artículo 18 del Decreto Supremo Nº 2514, dispone que: *"las entidades del sector público, en el marco de la Soberanía Tecnológica, deben designar un Responsable de Gobierno Electrónico y Tecnologías de Información y Comunicación y un Responsable de Seguridad Informática, encargados de coordinar con la AGETIC".*

Que, la Disposición Transitoria Segunda de esta referencia normativa, 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".*

Que, la Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, emitida por la AGETIC, en el marco del Artículo 7, inciso f) del Decreto Supremo Nº 2514, aprueba el documento "*Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público*"; norma administrativa de cumplimiento obligatorio para las entidades públicas.

Que, el punto 6.4 de los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", aprobada mediante Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, establece que: "*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.*"

Que, el Decreto Supremo N° 2765, de 14 de mayo de 2016, modifica la naturaleza jurídica de la Empresa Pública Nacional Textil-ENATEX, a Institución Pública Descentralizada, con duración indefinida, patrimonio propio, autonomía de gestión administrativa, financiera, legal y técnica, bajo tuición del Ministerio de Desarrollo Productivo y Economía Plural, cuya denominación es Servicio Nacional Textil-SENATEX.

Que, la Resolución Ministerial MDPyEP/DESPACHO/N° 172.2016, de fecha 15 de julio de 2016, emitida por el Ministerio de Desarrollo Productivo y Economía Plural, aprueba las atribuciones del Director General Ejecutivo de la Institución Pública Descentralizada Servicio Nacional Textil-SENATEX, el cual en su inciso g) prevé el emitir Resoluciones Administrativas en el marco de su competencia y conforme la norma vigente, fundamentadas por informe técnico legal.

Que, mediante Resolución Suprema N° 27306, de 04 de diciembre de 2020, se designa al ciudadano Gonzalo Benigno Uscamayta Gonzales como Director General Ejecutivo del Servicio Nacional Textil - SENATEX, a tuición del Ministerio de Desarrollo Productivo y Economía Plural.

Que, la Resolución Administrativa SENATEX/DGE/N° 0068/2023, de fecha 17 de octubre de 2023, en su artículo primero se dispuso la: "*...conformación del Comité de Seguridad de la Información -CSI del Servicio Nacional Textil - SENATEX, encargado de gestionar, promover e impulsar iniciativas en seguridad de la información en el marco de sus funciones previstas en*

los "Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", aprobada mediante Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, emitida por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC, la Ley N° 164, de 08 de agosto de 2011, el Decreto Supremo N° 2514, de 9 de septiembre de 2015,...".

CONSIDERANDO:

Que, a través de la Carta Externa AGETIC/NE/4057/2023, de 12 de septiembre de 2023, emitida por el Director General Ejecutivo de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, se solicita remitir hasta el 31 de octubre de 2023, el Plan Institucional de Seguridad de la Información aprobado, señalando que se tenga en cuenta la organización institucional, tal como se establecen en los lineamientos en relación a la designación y funciones del Responsable de Seguridad de la Información - RSI y de la conformación y funciones del Comité de Seguridad de la información - CSI.

Que, por Memorándum MEM/SENATEX/DGE Nº 0024/2023, se designó al Responsable de Seguridad de la Información – RSI y por Memorándum MEM/SENATEX/DGE Nº 0025/2023 se designó al Equipo de Apoyo del Responsable de Seguridad de la Información (RSI).

Que, mediante Informe Técnico INF/SENATEX/UGST N° 0299/2023, de 31 de octubre de 2023, la Unidad de Gestión de Servicios Técnicos, y la Unidad de Administración y Finanzas, señalan lo siguiente: "*Se elaboró y revisó el Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil - SENATEX.*" Por lo que, recomiendan: "*Remitir el presente informe a la Unidad de Asuntos Jurídicos para su correspondiente informe legal y elaboración de la Resolución Administrativa que apruebe el Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX (adjunto). Remitir una copia original para custodia de la Unidad de Gestión de Servicios Técnicos para la correspondiente difusión y remisión a la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC.*" A tal efecto adjunta copia del Memorándum MEM/SENATEX/DGE Nº 0024/2023, referente a la designación del Responsable de Seguridad de la Información – RSI, el Memorándum MEM/SENATEX/DGE Nº 0025/2023, sobre la designación del Equipo de Apoyo del Responsable de Seguridad de la Información (RSI) y el PISI antes mencionado.

Que, el Informe Legal INF/SENATEX/UAJ Nº 0177/2023, de fecha 31 de octubre de 2023, emitido en la Unidad de Asuntos Jurídicos del SENATEX, recomienda: "*Aprobar el Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX, mediante una Resolución Administrativa emanada de la Máxima Autoridad Ejecutiva del SENATEX, conforme a la atribución conferida por el inicio g) del Artículo 1 de la Resolución Ministerial MDPyEP/DESPACHO/N° 172.2016, de fecha 15 de julio de 2016, al encontrarse enmarcado en los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", aprobada mediante Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, emitida por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, la Ley N° 164, de 08 de agosto de 2011, el Decreto Supremo N° 2514, de 9 de septiembre de 2015 y demás normativa vigente.*"

SENATEX V°B° D.G.E. GONZALO USCAMAYTA GONZALES

POR TANTO:

El Director General Ejecutivo del Servicio Nacional Textil - SENATEX, en uso de sus atribuciones y facultades previstas por Ley.

UNIDAD DE ASUNTOS JURÍDICOS V°B° Z.G.M. SENATEX

RESUELVE:

HECHO EN BOLIVIA

PRIMERO: APROBAR el **Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX**, que en anexo forma parte integrante de la presente Resolución Administrativa.

SEGUNDO: ENCOMENDAR a la Unidad de Gestión de Servicios Técnicos del Servicio Nacional Textil – SENATEX, la difusión, ejecución y publicación del Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX, aprobado mediante la presente Resolución, en la página web del SENATEX.

TERCERO: INSTRUIR a Unidad de Gestión de Servicios Técnicos del Servicio Nacional Textil – SENATEX, remitir una copia fotostática debidamente legalizada del Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX a la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC).

REGÍSTRESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.

Gonzalo B. Uscamayta Gonzales
DIRECTOR GENERAL EJECUTIVO
SERVICIO NACIONAL TEXTIL
SENATEX

UNIDAD DE ASUNTOS JURIDICOS
V°B°
Z.G.M.
SENATEX

GBUG/ZGM
Cc. Archivo DGE/UAJ

HECHO EN BOLIVIA

INFORME LEGAL
INF/SENATEX/UAJ Nº 0177/2023
SENATEX-I/2023-05567

Gonzalo B. Uscamayta Gonzales
DIRECTOR GENERAL EJECUTIVO
SERVICIO NACIONAL TEXTIL
SENATEX

Zurly Garay Montoya
RESPONSABLE DE LA UNIDAD JURÍDICA
SERVICIO NACIONAL TEXTIL
SENATEX

A : Gonzalo Benigno Uscamayta Gonzales
DIRECTOR GENERAL EJECUTIVO

DE : Zurly Garay Montoya
RESPONSABLE DE LA UNIDAD DE ASUNTOS JURÍDICOS

REF. : **OPINIÓN LEGAL SOBRE LA APROBACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI) DEL SERVICIO NACIONAL TEXTIL – SENATEX.**

FECHA : La Paz, 31 de octubre de 2023.

En atención a la Hoja de Ruta SENATEX-I/2023-05567, tengo a bien elevar el presente Informe Legal, conforme lo siguiente:

1. ANTECEDENTES.

- A través de la Carta Externa AGETIC/NE/4057/2023, de 12 de septiembre de 2023, emitida por el Director General Ejecutivo de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, se solicita remitir hasta el 31 de octubre de 2023, el Plan Institucional de Seguridad de la Información aprobado, señalando que se tenga en cuenta la organización institucional, tal como se establecen en los lineamientos en relación a la designación y funciones del Responsable de Seguridad de la Información - RSI y de la conformación y funciones del Comité de Seguridad de la información - CSI.

- Por Memorándum MEM/SENATEX/DGE Nº 0024/2023, se designó al Responsable de Seguridad de la Información – RSI y por Memorándum MEM/SENATEX/DGE Nº 0025/2023 se designó al Equipo de Apoyo del Responsable de Seguridad de la Información (RSI).

- Mediante la Resolución Administrativa SENATEX/DGE/N° 0068/2023, de fecha 17 de octubre de 2023, en su artículo primero se dispuso la: "*... conformación del Comité de Seguridad de la Información -CSI del Servicio Nacional Textil - SENATEX, encargado de gestionar, promover e impulsar iniciativas en seguridad de la información en el marco de sus funciones previstas en los "Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", aprobada mediante Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, emitida por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC, la Ley N° 164, de 08 de agosto de 2011, el Decreto Supremo N° 2514, de 9 de septiembre de 2015,...*".

- Mediante Informe Técnico INF/SENATEX/UGST N° 0299/2023, de 31 de octubre de 2023, la Unidad de Gestión de Servicios Técnicos, y la Unidad de Administración y Finanzas, señalan lo siguiente: "*Se elaboró y revisó el Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil - SENATEX.*" Por lo que, recomiendan: "*Remitir el presente informe a la Unidad de Asuntos Jurídicos para su correspondiente informe legal y elaboración de la Resolución Administrativa que apruebe el Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX (adjunto). Remitir una copia original para custodia de la Unidad de Gestión de Servicios Técnicos para la correspondiente difusión y remisión a la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC.*" A tal efecto adjunta copia del Memorándum MEM/SENATEX/DGE Nº 0024/2023, referente a la designación del Responsable de Seguridad de la Información – RSI, el Memorándum MEM/SENATEX/DGE Nº 0025/2023, sobre la designación del Equipo de Apoyo del Responsable de Seguridad de la Información (RSI) y el PISI antes mencionado.

2. MARCO LEGAL:

La Constitución Política del Estado, en su Artículo 232, establece que: "*La Administración Pública se rige por los principios de legitimidad, legalidad, imparcialidad, publicidad, compromiso e interés social, ética, transparencia, igualdad, competencia, eficiencia, calidad, calidez, honestidad, responsabilidad y resultados.*".

El Parágrafo II del Artículo 103 del Texto Constitucional dispone 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*". El Parágrafo II de este mismo artículo, estipula que: "*El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de la información y comunicación*".

La Ley Nº 650, de 15 de enero de 2015, eleva a rango de Ley la "Agenda Patriótica del Bicentenario 2025", misma que en su Pilar 4 establece: "*Soberanía científica y tecnológica con identidad propia*".

El Artículo 71 de la Ley Nº 164, de 8 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación declara de prioridad nacional la promoción del uso de las tecnologías de información y comunicación para procurar el vivir bien de todas las bolivianas y bolivianos. Asimismo, el Parágrafo I del Artículo 72 de la citada Ley, 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.*"

SENATEX VºBº D.G.E. GONZALO USCAMAYTA GONZALES

UNIDAD DE ASUNTOS JURIDICOS VºBº Z.G.M. SENATEX

HECHO EN BOLIVIA

El Artículo 76 de la Ley Nº 164, determina 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.*"

El parágrafo II del Artículo 77 de la Ley Nº 164, de 8 de agosto de 2011, establece que "*...El Órgano Ejecutivo del nivel central del Estado, elaborará el plan de implementación de software libre y estándares abiertos en coordinación con los demás órganos del Estado y entidades de la administración pública.*"

El Artículo 2 del Decreto Supremo Nº 2514, de 9 de septiembre de 2015, dispone la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, como una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica, y patrimonio propio, bajo tuición del Ministerio de la Presidencia.

El parágrafo I del Artículo 8 del Decreto Supremo Nº 2514, crea el Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC, estableciendo dentro de sus funciones el de: "*c) Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público;* (...) *k) Realizar el seguimiento al desarrollo e implementación de los planes de seguridad de la información en las entidades y empresas públicas del nivel central del Estado; (...) y n) Realizar otras tareas orientadas a la mejora de la seguridad de la información de las entidades del sector Público.*"

El Parágrafo III del Artículo 17 del precitado Decreto Supremo, señala que: "*Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el Centro de Gestión de Incidentes Informáticos — CGII.*"

El Parágrafo II del Artículo 18 del Decreto Supremo Nº 2514, dispone que: "*las entidades del sector público, en el marco de la Soberanía Tecnológica, deben designar un Responsable de Gobierno Electrónico y Tecnologías de Información y Comunicación y un Responsable de Seguridad Informática, encargados de coordinar con la AGETIC*".

La Disposición Transitoria Segunda de esta referencia normativa, 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*".

SENATEX VoBº D.G.E. GONZALO USCAMAYTA GONZALES

UNIDAD DE ASUNTOS JURIDICOS VoBº Z.G.M. SENATEX

La Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, emitida por la AGETIC, en el marco del Artículo 7, inciso f) del Decreto Supremo Nº 2514, aprueba el documento "*Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público*"; norma administrativa de cumplimiento obligatorio para las entidades públicas.

HECHO EN BOLIVIA

El punto 6.4 de los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", aprobada mediante Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, establece que: "*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.*"

El Decreto Supremo N° 2765, de 14 de mayo de 2016, modifica la naturaleza jurídica de la Empresa Pública Nacional Textil-ENATEX, a Institución Pública Descentralizada, con duración indefinida, patrimonio propio, autonomía de gestión administrativa, financiera, legal y técnica, bajo tuición del Ministerio de Desarrollo Productivo y Economía Plural, cuya denominación es Servicio Nacional Textil-SENATEX.

La Resolución Ministerial MDPyEP/DESPACHO/N° 172.2016, de fecha 15 de julio de 2016, emitida por el Ministerio de Desarrollo Productivo y Economía Plural, aprueba las atribuciones del Director General Ejecutivo de la Institución Pública Descentralizada Servicio Nacional Textil-SENATEX, el cual en su inciso g) prevé el emitir Resoluciones Administrativas en el marco de su competencia y conforme la norma vigente, fundamentadas por informe técnico legal.

Mediante Resolución Suprema N° 27306, de 04 de diciembre de 2020, se designa al ciudadano Gonzalo Benigno Uscamayta Gonzales como Director General Ejecutivo del Servicio Nacional Textil - SENATEX, a tuición del Ministerio de Desarrollo Productivo y Economía Plural.

3. ANÁLISIS.

En mérito a los antecedentes arrimados y la normativa vigente, corresponde efectuar el siguiente análisis, conforme los siguientes puntos:

3.1. En atención a lo expuesto en el Informe INF/SENATEX/UGST N° 0299/2023, de acuerdo al punto 6.1.2 de los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", se evidencia que se dio cumplimiento a la designación del Responsable de Seguridad de la Información – RSI a través del Memorándum MEM/SENATEX/DGE Nº 0024/2023, y del Equipo de Apoyo del Responsable de Seguridad de la Información (RSI), por Memorándum MEM/SENATEX/DGE Nº 0025/2023, y se dispuso la conformación del Comité de Seguridad de la Información -CSI del Servicio Nacional Textil - SENATEX, con la Resolución Administrativa SENATEX/DGE/N° 0068/2023, de 17 de octubre de 2023, con la finalidad de la elaboración e implementación del PISI.

SENATEX V°B° D.G.E. GONZALO USCAMAYTA GONZALES

UNIDAD DE ASUNTOS JURIDICOS V°B° Z.A.M. SENATEX

3.2. Conforme lo denotado anteriormente se dio cumplimiento con la Etapa Inicial del PISI, por lo que de la revisión del documento del PISI, el mismo establece la etapa

HECHO EN BOLIVIA

del desarrollo del PISI, cuyo contenido contempla entre otros la adopción de metodología de gestión de riesgos, la identificación y clasificación de activos de información, valoración de activos de información, así como, los puntos mínimos con los que debe contar la Estructura de la Política de Seguridad de la Información, cronograma de implementación, conteniendo al efecto los requisitos descritos en el punto 6 de los de los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", aprobada mediante Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017.

3.3. En este sentido, acorde a los antecedentes vertidos y la normativa antes citada, no existe óbice legal para aprobar el Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX

3.4. En consecuencia, al existir viabilidad técnica, y lo solicitado se enmarca en la normativa vigente, no existe impedimento legal para que la Máxima Autoridad Ejecutiva del SENATEX, a través de una Resolución Administrativa apruebe el PISI, en virtud a la facultad descrita en al inicio g) del Artículo 1 de la Resolución Ministerial MDPyEP/DESPACHO/N° 172.2016, de fecha 15 de julio de 2016.

4. CONCLUSIONES.

De los antecedentes expuestos, la normativa legal aplicable y el análisis jurídico expresado en el presente Informe, se llegan a las siguientes conclusiones:

4.1. De acuerdo a los Memorándums MEM/SENATEX/DGE Nº 0024/2023, MEM/SENATEX/DGE Nº 0025/2023, se designó al Responsable de Seguridad de la Información – RSI y a su Equipo de Apoyo, asimismo, se dispuso la conformación del Comité de Seguridad de la Información -CSI del Servicio Nacional Textil - SENATEX, con la Resolución Administrativa SENATEX/DGE/N° 0068/2023, de 17 de octubre de 2023, dando cumplimiento a la etapa inicial del PISI, conforme lo dispuesto en los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público".

4.2. Respecto a la solicitud de aprobar el Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX, mediante una Resolución Administrativa, se concluye que no existe óbice legal para aprobar el mismo de acuerdo al punto 6.4 de los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público".

SENATEX V°B° D.G.E. ILO USCAMAYTA GONZALES

UNIDAD DE ASUNTOS JURIDICOS V° B° Z.G.M. SENATEX

5. RECOMENDACIÓN.

De los antecedentes, las disposiciones legales y la conclusión del presente informe, se **RECOMIENDA** a su Autoridad lo siguiente:

HECHO EN BOLIVIA

5.1. Aprobar el Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX, mediante una Resolución Administrativa emanada de la Máxima Autoridad Ejecutiva del SENATEX, conforme a la atribución conferida por el inicio g) del Artículo 1 de la Resolución Ministerial MDPyEP/DESPACHO/N° 172.2016, de fecha 15 de julio de 2016, al encontrarse enmarcado en los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público", aprobada mediante Resolución Administrativa AGETIC/RA/0051/2017, de 19 de septiembre de 2017, emitida por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, la Ley N° 164, de 08 de agosto de 2011, el Decreto Supremo N° 2514, de 9 de septiembre de 2015 y demás normativa vigente.

5.2. Encomendar a la Unidad de Gestión de Servicios Técnicos del Servicio Nacional Textil – SENATEX, la difusión, ejecución y publicación del Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX, aprobado mediante la presente Resolución, en la página web del SENATEX.

5.3. Instruir a la Unidad de Gestión de Servicios Técnicos del Servicio Nacional Textil – SENATEX, remitir una copia fotostática debidamente legalizada del Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX a la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC).

5.4. En ese sentido, se adjunta el proyecto de Resolución Administrativa recomendando que la misma sea suscrita por su Autoridad.

Es cuanto informo y recomiendo a su autoridad, para los fines consiguientes.

Zurly Geray Montoya
RESPONSABLE DE LA UNIDAD JURIDICA
SERVICIO NACIONAL TEXTIL
SENATEX

H.R.: SENATEX-I/2023-05567

SENATEX V°B° D.G.E. GONZALO USCAMAYTA GONZALES

ZGM

Cc./Archivo Unidad Jurídica.

HECHO EN BOLIVIA

INFORME

INF/SENATEX/UGST Nº 0299/2023

SENATEX-I/2023-05567

Gonzalo B. Uscamayta Gonzales
DIRECTOR GENERAL EJECUTIVO
SERVICIO NACIONAL TEXTIL
SENATEX

A : Gonzalo Benigno Uscamayta Gonzales
DIRECTOR GENERAL EJECUTIVO

DE : Lobsang Roger Ferrufino Rojas
JEFE DE LA UNIDAD DE GESTIÓN DE SERVICIOS TÉCNICOS

Cesar José Moya Vargas
JEFE DE LA UNIDAD DE ADMINISTRACIÓN Y FINANZAS

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI)

REF : **Aprobación del Plan Institucional de Seguridad de la Información – PISI del Servicio Nacional Textil - SENATEX**

FECHA : La Paz, 31 de octubre de 2023

1. ANTECEDENTES.

Nota Externa AGETIC/NE/4057/2023 de fecha 13 de septiembre de 2023 remitida con Hoja de Ruta Externa SENATEX-E/2023-04725 con referencia "ELABORACIÓN PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN"

Memorándum MEM/SENATEX/DGE Nº 0024/2023 con referencia designación al Responsable de Seguridad de la Información – RSI.

Memorándum MEM/SENATEX/DGE Nº 0025/2023 con referencia designación al Equipo de Apoyo del Responsable de Seguridad de la Información (RSI).

Resolución Administrativa SENATEX/DGE/N° 0068/2021 de fecha 17 de octubre de 2023, que conforma el Comité de Seguridad de la Información (CSI).

2. MARCO LEGAL.

El inciso t) del Artículo 22 del Decreto Supremo No 29894, de 7 de febrero de 2009, de Organización del Órgano Ejecutivo, que establece que: "El Ministerio de la Presidencia es el ente rector de Gobierno Electrónico y de Tecnologías de Información y Comunicación para el sector público del Estado Plurinacional de Bolivia, siendo el encargado de establecer las políticas, lineamientos y normativa específica para su implementación, seguimiento y control".

El inciso d) del Artículo 4 (Principios), parágrafo II, del Decreto Supremo N° 1793 de 13 de noviembre de 2013, que señala que: "Se debe implementar los controles técnicos y

HECHO EN BOLIVIA

administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravió, utilización y acceso no autorizado o fraudulento".

El Artículo 8 (Plan de contingencia) del citado cuerpo legal, que menciona que: "Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad".

El Artículo 2 del Decreto Supremo N° 2514, de 9 de septiembre de 2015, sobre la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC, como "una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica y patrimonio propio, bajo tuición del Ministerio de la Presidencia.

Lo señalado en los artículos 9, 10 y 11 del citado cuerpo legal, acerca de la creación del Consejo para las Tecnologías de Información y Comunicación para formular y presentar propuestas de políticas, normativa, programas y proyectos de Gobierno Electrónico y Tecnologías de Información y Comunicación por parte de las entidades del ámbito gubernamental.

Inciso f) del Artículo 7 del citado cuerpo legal, que sostiene que la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) establecerá los lineamientos técnicos en seguridad de información para las entidades del sector público".

Inciso i) del Artículo 7 del citado cuerpo legal, que establece entre las funciones de la AGETIC, "Elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática".

Parágrafo I del Artículo 8 del citado cuerpo legal, 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 del citado cuerpo legal, que menciona como una de las funciones del Centro de Gestión de Incidentes Informáticos – CGII, "Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público".2

Parágrafo III del Artículo 17 del citado cuerpo legal, que establece que "Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII".

Parágrafo II del Artículo 18 del citado cuerpo legal, que señala que "Las entidades del sector público, en el marco de la Soberanía Tecnológica, deben designar un Responsable de

Calle Yanacachi N°1489, Zona Villa Fátima. Telf.: (591-2) 219595
La Paz – Bolivia
www.senatex.gob.bo

Gobierno Electrónico y Tecnologías de Información y Comunicación un Responsable de Seguridad Informática, encargados de coordinar con la AGETIC".

Disposición transitoria segunda, que sostiene 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".

El Artículo 2, del Decreto Supremo N° 2765, de fecha 14 de mayo de 2016, modifica la naturaleza jurídica de ENATEX, de Empresa Pública Nacional Estratégica - EPNE a Institución Pública Descentralizada, con duración indefinida, patrimonio propio, autonomía de gestión administrativa, financiera, legal y técnica, bajo tuición del Ministerio de Desarrollo Productivo y Economía Plural, cuya denominación a partir de la fecha será Servicio Nacional Textil – SENATEX, sujeta al régimen legal de la Ley N° 2027, de 27 de octubre de 1999, Estatuto del Funcionario Público, Ley N° 1178, de 20 de julio de 1990, de Administración y Control Gubernamentales y demás normativa aplicable a la Administración Pública.

El Artículo 3, del mencionado Decreto Supremo, dispone como competencia institucional del Servicio Nacional Textil – SENATEX, impulsar el cambio de la matriz productiva nacional a través del incremento de la agregación de valor a la producción primaria, transformación tecnológica, alza de la productividad, diversificación productiva y mayor generación de excedentes e ingresos en la producción textil, participando en la creación, consolidación, modernización y tecnificación de los emprendimientos productivos textiles del país.

El Artículo 5, de la citada disposición legal, establece las funciones del Servicio Nacional Textil – SENATEX, entre las cuales se encuentran:

1. Producir, transformar y comercializar productos e insumos textiles en el mercado interno y/o externo;
2. Comprar de manera directa en el mercado interno y/o importar materias primas e insumos, para la provisión propia y/o de las Unidades Productivas textiles del país;
3. Realizar la exportación de productos textiles con valor agregado;
4. Gestionar mercados internos y/o externos para productos e insumos textiles;
5. Prestar servicios tecnológicos a las unidades productivas textiles;
6. Realizar ensayos de laboratorio para la Evaluación de la Conformidad;
7. Apoyar las políticas para el desarrollo del sector textil nacional;
8. Gestionar y apoyar la elaboración de planes de negocios de Unidades Productivas Textiles;
9. Administrar y ejecutar recursos públicos, provenientes de la cooperación internacional;
10. Suscribir convenios en el ámbito de sus funciones;

HECHO EN BOLIVIA

Calle Yanacachi N°1489, Zona Villa Fátima. Telf.: (591-2) 219595
La Paz – Bolivia
www.senatex.gob.bo

11. Todas las demás funciones que sean necesarias para el cumplimiento de su competencia institucional.

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.

3. DESARROLLO

Según los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público, se indica en el punto 6 Lineamientos para elaboración del PISI se describe el Proceso de Elaboración de PISI por Etapas, del cual se divide en dos: i) Etapa Inicial y ii) Etapa de Desarrollo.

Por lo tanto, la ETAPA INICIAL tiene por objetivo contar con una Organización Interna en la institución pública, asimismo, en orden al inciso d) del punto 6.1.1. Responsabilidades de la Máxima Autoridad Ejecutiva (MAE) respecto a la seguridad de la información, debe realizar las siguientes actividades:

3.1. Designación del Responsable de Seguridad de la Información

Realizada mediante Memorándum N° MEM/SENATEX/DGE Nº 0024/2023. Adicionalmente, se designó al **Equipo de Apoyo del Responsable de Seguridad de la Información (RSI)**, realizada mediante Memorándum N° MEM/SENATEX/DGE Nº 0025/2023.

3.2. Conformación del Comité de Seguridad de la Información

En orden al punto 6.1.3. Conformación y funciones del Comité de Seguridad de la Información (CSI) de los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público, la MAE designará al personal que conformará el Comité de Seguridad de la Información (CSI) mediante resolución administrativa, la misma fue emitida mediante Resolución Administrativa SENATEX/DGE/N° 0068/2021 de fecha 17 de octubre de 2023, que conforma el Comité de Seguridad de la Información (CSI)

Conforme a los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público, 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.

HECHO EN BOLIVIA

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.

Por lo tanto, en orden a los incisos a y b indicados precedentemente, se da anuencia a la implementación del Plan Institucional de Seguridad de la Información (PISI) del SENATEX.

Consecuentemente, una vez se cuente con la aprobación del PISI en nuestra calidad de Comité de Seguridad de la Información (CSI) en coordinación con el Responsable de Seguridad (RSI) de la Información somos encargados de verificar la correcta implementación, aplicación y cumplimiento.

4. CONCLUSIÓN

De los antecedentes y normativa expuesta, se establece las siguientes conclusiones:

4.1. Se designó al **Responsable de Seguridad de la Información – RSI** mediante Memorándum MEM/SENATEX/DGE Nº 0024/2023.

4.2. Se designó al Equipo de Apoyo del Responsable de Seguridad de la Información (RSI) mediante Memorándum MEM/SENATEX/DGE Nº 0025/2023.

4.3. Se conformó al Comité de Seguridad de la Información (CSI) mediante Resolución Administrativa SENATEX/DGE/N° 0068/2021 de fecha 17 de octubre de 2023.

4.4. Se elaboró y revisó el Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil - SENATEX.

5. RECOMENDACIÓN

Recomendación 1. Remitir el presente informe a la Unidad de Asuntos Jurídicos para su correspondiente informe legal y elaboración de la Resolución Administrativa que apruebe el **Plan Institucional de Seguridad de la Información (PISI) del Servicio Nacional Textil – SENATEX** (adjunto)**.**

Calle Yanacachi N°1489, Zona Villa Fátima. Telf.: (591-2) 219595
La Paz – Bolivia
www.senatex.gob.bo

Recomendación 2. Remitir una copia original para custodia de la Unidad de Gestión de Servicios Técnicos para la correspondiente difusión y remisión a la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC.

Es cuanto informo para fines consiguientes:

Ing. Roger Fernando Rojas
JEFE DE LA UNIDAD DE GESTIÓN DE SERVICIOS TECNICOS
SENATEX

Ing. César José Moya Vargas
JEFE DE LA UNIDAD DE ADMINISTRACIÓN Y FINANZAS
SERVICIO NACIONAL TEXTIL
SENATEX

LRFR/CJMV/aaci/bkss
cc: Arch. UGST
Adj: Lo indicado

HECHO EN BOLIVIA

BICENTENARIO DE BOLIVIA

SENATEX
SERVICIO NACIONAL TEXTIL

ESTADO PLURINACIONAL DE BOLIVIA
MINISTERIO DE DESARROLLO PRODUCTIVO Y ECONOMÍA PLURAL

2023

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN P.I.S.I.

Unidad de Gestión de Servicios Técnicos
UGST

PI-UGST-PISI-003

(591-2) 2219595
www.senatex.gob.bo
www.facebook.com/senatex.bolivia

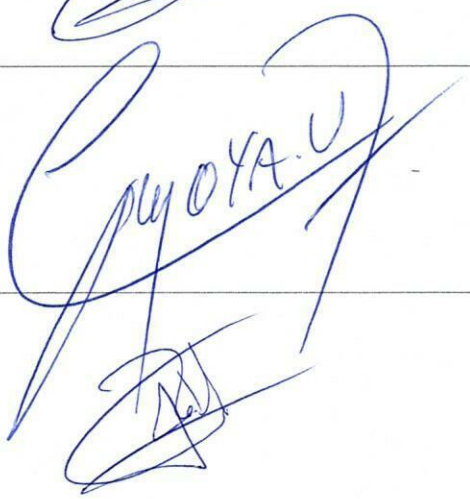
SENATEX V°B° U.G.S.T.

SENATEX V°B° A.A.C.I. TECNICO SOPORTE DE SISTEMAS

SENATEX V°B° U.R.S.S. PROFESIONAL EN ORGANIZACION ADMINISTRATIVA

SENATEX V°B° D.G.E. GONZALO USCAMAYTA GONZALES

CONTROL DEL DOCUMENTO

	FIRMA	SELLO
APROBACIÓN		Gonzalo B. Uscamayta Gonzales DIRECTOR GENERAL EJECUTIVO SERVICIO NACIONAL TEXTIL SENATEX
REVISIÓN		Lobsang Roger Ferrufino Rojas JEFE DE LA UNIDAD DE GESTIÓN DE SERVICIOS TECNICOS SENATEX
REVISIÓN		Lic. César José Moya Vargas JEFE DE LA UNIDAD DE ADMINISTRACIÓN Y FINANZAS SERVICIO NACIONAL TEXTIL SENATEX
ELABORACIÓN		Lobsang Roger Ferrufino Rojas JEFE DE LA UNIDAD DE GESTIÓN DE SERVICIOS TECNICOS SENATEX
ELABORACIÓN		Abimael Alvaro Choque Ingala TECNICO EN SOPORTE DE SISTEMAS SERVICIO NACIONAL TEXTIL SENATEX
ELABORACIÓN		Lic. Brenda K. Soruco Salazar PROFESIONAL EN ORGANIZACIÓN ADMINISTRATIVA SERVICIO NACIONAL TEXTIL - SENATEX

CONTENIDO

CAPITULO I
GENERALIDADES

1.1. INTRODUCCIÓN

Las nuevas tecnologías de información y comunicación (TIC) han revolucionado la forma en que las personas, las empresas y las instituciones interactúan con el mundo digital. Estas innovaciones permiten a individuos y organizaciones enviar y recibir información de diversa índole con una facilidad sin precedentes, siempre y cuando tengan acceso a una terminal de comunicación. Las posibilidades que brindan las TIC son verdaderamente ilimitadas, ya que no solo facilitan la comunicación, sino que también posibilitan la realización de trabajos de alta precisión y funciones vitales para las instituciones en diversos sectores, desde la educación y la salud hasta la administración gubernamental y la investigación científica.

A pesar de las numerosas ventajas que ofrecen las TIC, es imperativo reconocer que también conllevan una serie de amenazas que son globales en alcance y varían en nivel de criticidad según el enfoque y el ámbito en el que se utilicen. Cada día surgen nuevos métodos y tácticas que pueden poner en peligro la seguridad de la información de las organizaciones, lo que subraya la necesidad de establecer una estrategia completa de seguridad. Estas amenazas no solo provienen del exterior, sino que también se relacionan con vulnerabilidades internas, que representan un riesgo significativo para la integridad de la información.

Por lo tanto, es fundamental contar con normas y procedimientos efectivos que permitan prevenir y, en caso necesario, corregir posibles ataques y amenazas que puedan comprometer la integridad, la confidencialidad y la disponibilidad de la información. La seguridad de las TIC se ha convertido en una prioridad en el entorno digital actual, y su gestión adecuada no solo protege los activos y datos de una organización, sino que también garantiza la confianza de los usuarios y la continuidad de las operaciones en un mundo cada vez más interconectado y dependiente de la tecnología.

Consecuentemente, el Plan Institucional de Seguridad de la Información – PISI del SENATEX es un componente crucial en la gestión de la seguridad de la información. Este plan es una estrategia integral que se desarrolla para proteger los activos de información, garantizar la confidencialidad, integridad y disponibilidad de los datos, y mitigar los riesgos asociados a las amenazas tanto internas como externas.

El Plan Institucional de Seguridad de la Información del SENATEX, muestra de forma clara la intención de cumplir con los objetivos planteados, para lo cual, presenta en forma esquematizada: i) Descripción Preliminar de la Entidad indicando los Antecedentes de la institución, Marco Normativo, Estructura Organizacional, Objetivos y Alcance del SENATEX; ii) Metodología de gestión de riesgos, iii) Política de Seguridad de la Información y iv) Cronograma de implementación.

1.2. DIAGNOSTICO INSTITUCIONAL

1.2.1. ANTECEDENTES DE LA INSTITUCIÓN

En fecha 12 de marzo de 2015, el gobierno con base al Estudio de Identificación del Proyecto "Ampliación de la Capacidad Productiva de la Empresa Nacional Pública" aprueba el Decreto Supremo N.º 2290 autorizando la asignación de recursos por un monto de Bs 142.154.325,00 del "Fondo para la Revolución Industrial Productiva" – FINPRO, estableciendo un plazo de 16 años, con 3 años de gracia a capital e interés.

Bajo este contexto, el Decreto Supremo 2765 del 14 de mayo de 2016, que modifica la naturaleza jurídica de ENATEX, de Empresa Pública Nacional Estratégica EPNE a institución Pública Descentralizada, con duración indefinida, patrimonio propio, autonomía de gestión administrativa, financiera, legal y técnica, bajo tuición del Ministerio de Desarrollo Productivo y Economía plural, cuya denominación a partir de la fecha será Servicio Nacional Textil.

El Servicio Nacional Textil - SENATEX está destinado a impulsar el cambio de la matriz productiva nacional a través del incremento de la agregación de valor a la producción primaria, transformación tecnológica, alza de la productividad, diversificación productiva y mayor generación de excedentes e ingresos en la producción textil, participando en la creación, consolidación, modernización y tecnificación de los emprendimientos productivos textiles del país.

El Servicio Nacional Textil - SENATEX, tiene las siguientes funciones:

- Producir, transformar y comercializar productos e insumos textiles en el mercado interno y/o importar materias primas e insumos, para la provisión propia y/o de las Unidades Productivas textiles del país.
- Realizar la exportación de productos textiles con valor agregado.
- Gestionar mercados internos y/o externos para productos e insumos textiles.
- Prestar servicios tecnológicos a las Unidades Productivas Textiles.
- Realizar ensayos de laboratorio para la Evaluación de la conformidad.
- Apoyar las políticas para el desarrollo del sector textil nacional.
- Gestionar y apoyar la elaboración de planes de negocios de Unidades productivas Textiles.
- Administrar y ejecutar recursos públicos, provenientes de la cooperación internacional.
- Suscribir convenios en el ámbito de sus funciones.

- Todas las demás funciones que sean necesarias para el cumplimiento de su competencia institucional.

1.2.2. MARCO ESTRATÉGICO

1.2.2.1. MISIÓN

Impulsar el cambio de la matriz productiva nacional a través del incremento de la agregación de valor a la producción primaria, transformación tecnológica, alza de la productividad, diversificación productiva y mayor generación de excedentes e ingresos en la producción textil, participando en la creación, consolidación, modernización y tecnificación de los emprendimientos productivos textiles del país.

1.2.2.2. VISIÓN

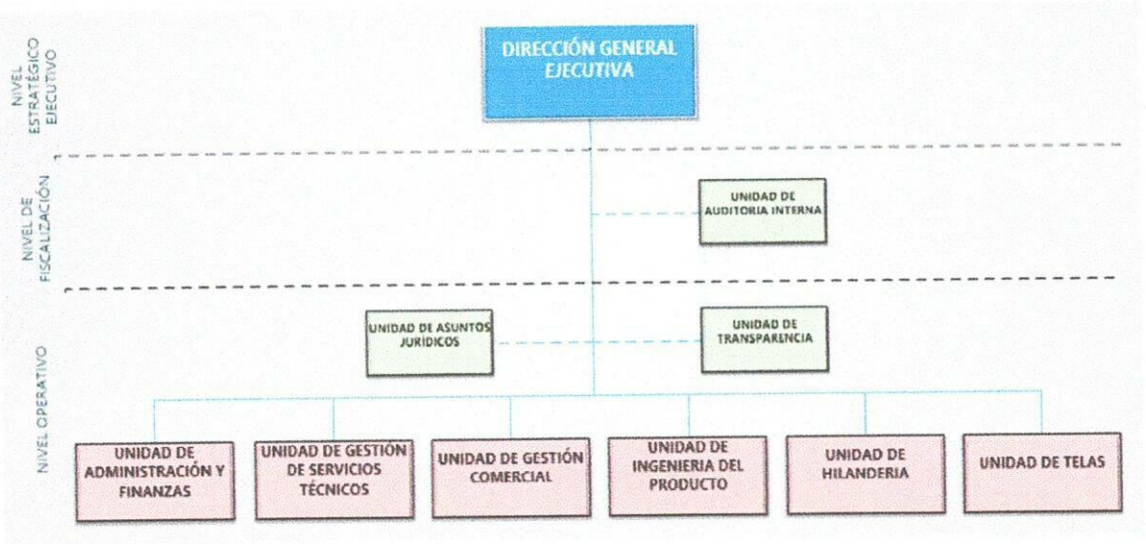
Ser el Servicio Nacional líder del Estado boliviano, motor principal y dinamizador del Complejo Productivo Textil, eficaz, eficiente y proactivo con proyección y presencia nacional e internacional.

1.2.2.3. OBJETIVOS ESTRATÉGICOS INSTITUCIONALES

- Apoyar a la producción nacional en el sector textil que sustituyen importaciones.
- Impulsar nuevas líneas de producción textil nacional hacia la sustitución de importaciones.
- Incrementar la venta de hilos, telas y prendas de vestir en el mercado interno y externo.
- Elevar el nivel del sector textil del país, por medio de la capacitación y el acceso a servicios especializados de hilatura, tejeduría, embellecimiento, laboratorio.
- Impulsar nuevas líneas de producción textil nacional hacia la sustitución de importaciones.
- Generar excedentes para lograr el pago de las cuotas de los fideicomisos y lograr el mantenimiento, reposición y/o adquisición de maquinaria.

1.2.3. ESTRUCTURA ORGANIZACIONAL

La Estructura Organizacional actual del SENATEX, es la siguiente:



Fuente: Unidad de Gestión de Servicios Técnicos.

Es importante mencionar que la Unidad de Gestión de Servicios Técnicos es la encargada de organizar y supervisar los sistemas informáticos del SENATEX, a través de su área de Sistemas.

1.3. MARCO NORMATIVO

Conforme al documento "*Lineamientos para la elaboración e implementación de los planes institucionales de seguridad de la información de las entidades del sector público*" el marco normativo referencial se enmarca en:

Mandato institucional respaldado por:

- El inciso t) del Artículo 22 del Decreto Supremo No 29894, de 7 de febrero de 2009, de Organización del Órgano Ejecutivo, que establece que: "El Ministerio de la Presidencia es el ente rector de Gobierno Electrónico y de Tecnologías de Información y Comunicación para el sector público del Estado Plurinacional de Bolivia, siendo el encargado de establecer las políticas, lineamientos y normativa específica para su implementación, seguimiento y control".
- El Artículo 2 del Decreto Supremo N° 2514, sobre la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC, como "una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica y patrimonio propio, bajo tuición del Ministerio de la Presidencia.

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

El marco normativo concerniente a la seguridad de la información incluye:

- El Parágrafo I del Artículo 72 de la Ley N° 164 de 28 de julio de 2011, Ley General de Telecomunicaciones, que establece que: "El Estado en todos sus niveles, fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, el despliegue y uso de infraestructura, el desarrollo de contenidos y aplicaciones, la protección de las usuarias y usuarios, la seguridad informática y de redes, como mecanismos de democratización de oportunidades para todos los sectores de la sociedad y especialmente para aquellos con menores ingresos y con necesidades especiales".
- El inciso d) del Artículo 4 (Principios), parágrafo II, del Decreto Supremo N° 1793 de 13 de noviembre de 2013, que señala que: "Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravió, utilización y acceso no autorizado o fraudulento".
- El Artículo 8 (Plan de contingencia) del Decreto Supremo N° 1793, de 13 de noviembre de 2013, que menciona que: "Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad".
- El Decreto Supremo N° 2514 de 9 de septiembre de 2015, en los siguientes artículos, incisos o disposiciones transitorias:
  - Inciso f) del Artículo 7, que sostiene que la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) establecerá los lineamientos técnicos en seguridad de información para las entidades del sector público".
  - Inciso i) del Artículo 7, que establece entre las funciones de la AGETIC, "Elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática".
  - Parágrafo I del Artículo 8, de creación del "Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC".

- Inciso c) del Parágrafo II del Artículo 8, que menciona como una de las funciones del Centro de Gestión de Incidentes Informáticos – CGII, "Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público".2
- Parágrafo III del Artículo 17, que establece que "Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII".
- Parágrafo II del Artículo 18, que señala que "Las entidades del sector público, en el marco de la Soberanía Tecnológica, deben designar un Responsable de Gobierno Electrónico y Tecnologías de Información y Comunicación un Responsable de Seguridad Informática, encargados de coordinar con la AGETIC".
- Disposición transitoria segunda, que sostiene 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".

- 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.

1.4. TÉRMINOS Y DEFINICIONES

a) **Activo:** En general, es todo aquello que tiene valor para la entidad o institución pública.

b) **Activo de Información:** Conocimientos o datos que tienen valor para la institución.

c) **Administración de Riesgos:** Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

d) **Amenaza:** Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en una organización. Riesgo: Combinación de la probabilidad de un evento adverso y su consecuencia.

e) **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

f) **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

g) **Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

h) **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos autorizados. Asimismo, se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

i) **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

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

k) **Claves criptográficas:** Algunos de los ejemplos de activos en esta categoría son: claves para cifrar, firmar, certificados x509, entre otros.

l) **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

m) **Equipamiento auxiliar:** En esta categoría están: fuentes de alimentación, generadores eléctricos, equipos de climatización, cableado eléctrico, mobiliario, entre otros.

n) **Equipamiento informático (Hardware):** En esta categoría están los medios físicos que soportan los procesos como ser: servidores, equipamiento de escritorio, periféricos, dispositivos de red perimetral, dispositivos de red, corta fuegos, entre otros.

o) **Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

p) **Incidente de Seguridad:** Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

q) **Información:** En esta clasificación ingresan procesos relevantes para la institución e información en cualquier medio de soporte físico o digital. Los

tipos de información que ingresarían son: información estratégica, información relacionada con el archivo personal, información relacionada a la documentación administrativa, legal, procesos de adjudicación y otros que tengan un coste económico y de cumplimiento con la normativa legal. También, en esta categoría está la información de archivos tales como respaldos, documentos, credenciales de acceso, entre otros.

r) **Instalaciones:** Edificio, vehículos, instalaciones de refuerzo, entre otros.

s) **Integridad:** Propiedad de salvaguardar la exactitud, totalidad de la información, los métodos de procesamiento y completitud de los activos. Disponibilidad: Propiedad de ser accesible y utilizable por solicitud de una entidad autorizada.

t) **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

u) **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

v) **Personal:** Incluye personal fijo, eventual, terceros, entre otros. También se debe identificar a los responsables y custodios de la información asociada al activo; esto es importante porque a través de la identificación se realizará una mejor valoración para resguardar la información. Los custodios podrían ser los mismos servidores públicos o en otros casos una persona ajena a la entidad o institución pública.

w) **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

x) **Redes de comunicaciones:** Están los servicios de comunicaciones como ser: la red telefónica, redes de datos, internet, entre otros.

y) **Responsable de Seguridad Informática:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

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

aa) **Servicios:** En esta categoría ingresan: servicios de acceso remoto, transferencia de archivos, correo electrónico, servicios web, servicio de directorio, entre otros.

bb) Seguridad de la Información: La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

cc) Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

dd) Software – aplicaciones informáticas: En esta categoría se encuentran: sistemas desarrollados y/o adquiridos, software de aplicación, sistemas operativos, software de virtualización, entre otros.

ee) Soportes de información: En esta categoría están: discos virtuales y físicos, memorias USB, discos y cintas, material impreso, entre otros.

ff) Tecnología de la Información: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

gg) Vulnerabilidad: Debilidad de un activo o control, que puede ser explotada por una amenaza. Impacto: Cambio adverso en la operación normal de un proceso de la institución pública.

1.5. OBJETIVOS

1.5.1. OBJETIVO GENERAL

Fortalecer la seguridad de la información en la organización, garantizando la confidencialidad, integridad y disponibilidad de los datos, así como la continuidad de las operaciones, a través de la implementación de políticas, procedimientos y medidas de seguridad efectivas, la concienciación del personal, y una respuesta eficiente a incidentes, con el fin de mitigar las amenazas internas y externas en el entorno de las tecnologías de información y comunicación.

1.5.2. OBJETIVOS ESPECÍFICOS

a) Desarrollar un inventario completo de activos de información del SENATEX e identificar un responsable que vele por su disponibilidad, confidencialidad e integridad.

b) Clasificar la información en función de su importancia y nivel de sensibilidad, lo que permitirá aplicar medidas de seguridad proporcionales.

c) Establecer normativa clara y comprensible que regulen el uso de sistemas y datos, y asegurarse de que todo el personal lo conozca y cumpla.

d) Establecer sistemas de control de acceso para garantizar que solo las personas autorizadas tengan acceso a la información sensible.

e) Realizar evaluaciones de riesgos regulares periódicos para identificar amenazas y vulnerabilidades emergentes y actualizar las medidas de seguridad en consecuencia.

f) Promover la formación y concienciación del personal sobre prácticas seguras en el uso de tecnologías de la información y la importancia de la seguridad de la información.

g) Evaluar y seleccionar soluciones de seguridad tecnológica.

h) Promover una cultura organizativa en la que la seguridad de la información sea una prioridad para todo el personal del SENATEX.

1.6. ALCANCE

El Plan Institucional de Seguridad de la Información – PISI, tiene como alcance a todas las unidades organizacionales del SENATEX, expuestos en el punto 1.2.3. precedente; incluyendo, pero no limitándose a, los siguientes aspectos:

i. **Activos de Información:** abarca la protección de todos los activos de información crítica de la organización, incluyendo datos, sistemas, aplicaciones, infraestructura de red, hardware y software.

ii. **Personal:** incluye a todos los empleados, contratistas, proveedores y cualquier otra entidad que tenga acceso a los activos de información de la institución.

iii. **Políticas y Procedimientos:** abarca el desarrollo, implementación y mantenimiento de políticas y procedimientos relacionados con la seguridad de la información, incluyendo políticas de acceso, contraseñas, gestión de incidentes, clasificación de datos, entre otras.

iv. **Tecnología:** Incluye la seguridad de la infraestructura tecnológica de la organización, lo que abarca sistemas operativos, bases de datos, redes, servidores y cualquier otra tecnología utilizada para el almacenamiento, procesamiento y transmisión de datos.

v. **Concienciación y Formación:** aborda programas de formación y concienciación destinados a todos los miembros de la institución para promover una cultura de seguridad de la información.

vi. **Auditorías y Evaluaciones:** incluye la realización de auditorías internas y evaluaciones regulares para medir el cumplimiento de las políticas de seguridad y la efectividad de las medidas de seguridad implementadas.

vii. **Respuesta a Incidentes:** cubre la preparación y respuesta a incidentes de seguridad de la información, lo que involucra la identificación, gestión, comunicación y recuperación de incidentes de seguridad.

viii. **Mejora Continua:** abarca la revisión periódica de políticas, procedimientos y medidas de seguridad, así como la identificación y aplicación de mejoras basadas en evaluaciones y cambios en el entorno de seguridad.

ix. **Cumplimiento Legal y Regulatorio:** asegura el cumplimiento de todas las leyes y regulaciones pertinentes relacionadas con la seguridad de la información que afecten a la organización.

x. **Relaciones con Terceros:** incluye la seguridad de la información en las relaciones con proveedores, clientes y otras partes externas que interactúan con la institución.

Por lo tanto, los descritos precedentemente garantizarán que el PISI abarque todos los aspectos críticos de la seguridad de la información en el SENATEX y permita la protección adecuada de los activos de información, la gestión de riesgos y la promoción de una cultura de seguridad.

1.7. REVISIÓN Y ACTUALIZACIÓN

El Responsable de Seguridad de la Información (RSI), el Comité de Seguridad de la Información (CSI) y la Unidad de Gestión de Servicios Técnicos a través del Equipo de apoyo del RSI revisará el presente Reglamento, cuando corresponda se ajustará y actualizará acorde a las necesidades de la institución y, la normativa vigente y aplicable al efecto, considerando los siguientes:

i. El análisis y/o evaluación de la experiencia derivada de su aplicación.

ii. Según las necesidades estructurales que se presenten.

iii. Por los cambios que pueda haber en las disposiciones legales.

iv. Por necesidades emergentes de las observaciones y/o recomendaciones fundamentadas que surjan dentro la entidad.

1.8. APROBACIÓN Y VIGENCIA

El presente plan entrará en vigencia desde la fecha de su aprobación mediante Resolución Administrativa, dejando sin efecto la normativa antepuesta. Siendo responsables de su correcta aplicación, implementación y control, el Responsable de Seguridad de la Información (RSI), el Comité de Seguridad de la Información (CSI) y la Unidad de Gestión de Servicios Técnicos, en lo que corresponda.

1.9. DIFUSIÓN

El Responsable de Seguridad de la Información (RSI), el Comité de Seguridad de la Información (CSI) y la Unidad de Gestión de Servicios Técnicos a través del Equipo de apoyo

del RSI gestionará la oportuna publicación en la página web e implementación correspondiente.

1.10. INCUMPLIMIENTO

El incumplimiento con lo establecido en el presente Reglamento, será sancionado de acuerdo a lo establecido en el Decreto Supremo 23318-A Reglamento de la Responsabilidad por la Función Pública, Reglamento Interno de Personal y normativa vigente.

1.11. SEGURIDAD Y PREVISIÓN

En caso de existir omisiones y contradicciones o diferencias en la interpretación del presente Reglamento, las mismas serán solucionadas dentro de los alcances y previsiones de la normativa de mayor jerarquía.

CAPITULO II
ETAPA INICIAL DEL PISI

2.1. ORGANIZACIÓN INTERNA

Comienza por la designación del Responsable de Seguridad de la Información (RSI) mediante memorándum correspondiente y la conformación del Comité de Seguridad de la Información (CSI) mediante Resolución Expresa 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.

2.2. RESPONSABILIDADES DE LA MÁXIMA AUTORIDAD EJECUTIVA (MAE)

Respecto a la seguridad de la información, en orden a los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público, la MAE 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.

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

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

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 institución.

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

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

2.1. FUNCIONES DEL RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (RSI)

El RSI tiene 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 institución.

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

2.2. FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI)

El CSI asume 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 institución.

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.

CAPITULO III
ETAPA DE DESARROLLO DEL PISI

3.1. GESTIÓN DE RIESGOS

3.1.1. ADOPCIÓN DE METODOLOGÍA

Con el fin de adoptar una metodología de gestión de riesgos, el SENATEX empleará la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT Versión 3, un método sistemático que implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que las medidas de control sean más adecuadas permitiendo tener riesgos mitigados en el PISI.

En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que la institución tome decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Por consiguiente, persigue los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

MAGERIT como metodología de gestión de riesgos, incorpora los siguientes aspectos: i) Identificación, clasificación y valoración de activos de información, ii) Evaluación del riesgo, iii) Tratamiento del riesgo y iv) Controles implementados y por implementar.

La metodología indicada nos ayudará a implementar controles de seguridad de información y mejorar la eficacia de los controles existentes, así también, nos ayudará a identificar acciones que contribuyan al correcto tratamiento de los riesgos, los cuales contribuirán al cumplimiento de los objetivos institucionales planteados.

3.1.2. IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

La identificación de activos de información permitirá al SENATEX clasificar y valorar el activo en términos cualitativos y cuantitativos, para brindar mejor tratamiento y protección, en este sentido del RSI conjuntamente con los responsables de estos activos, deberán asegurarse que se tenga la documentación actualizada de la institución , para ello se deberá realizar reuniones con el personal involucrado e identificar los activos de información en función a los alcances definidos en el presente plan.

A continuación, se muestra una tabla de clasificación de los activos que se manejara en el SENATEX.

Tabla 1. CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DEL SENATEX

NOMENCLATURA	TIPO DE ACTIVO	DESCRIPCIÓN
INF	Datos o Información	En esta clasificación ingresan procesos relevantes para la institución en información en cualquier medio de soporte físico o digital. Los tipos de información que ingresarían son: información estratégica, información relacionada con el archivo personal, información relacionada a la documentación administrativa, legal, procesos de adjudicación y otros que tengan un coste económico cumplimiento con la normativa legal. También, en esta categoría esta la información de archivos tales como respaldos, documentos, credenciales de acceso, entre otros.
K	Claves criptográficas	La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos. En esta categoría ingresan: claves para cifrar, firmar, entre otros.
S	Servicios	En esta categoría ingresan: servicios de acceso remoto, transferencia de archivos, correo electrónico, servicios web, servicio de directorio, entre otros.
SW	Software-Aplicaciones Informáticas	En esta categoría se encuentran: sistemas desarrollados y/o adquiridos, software de aplicación, sistemas operativos, software de virtualización, entre otros. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.
HW	Equipamiento Informático (HARDWARE)	En esta categoría están los medios físicos que soportan los procesos como ser: servidores, equipamiento de escritorio, periféricos, dispositivos de red perimetral, dispositivos de red, corta fuegos, entre otros.
COM	Redes de comunicaciones	Están los servicios de comunicaciones como ser: la red telefónica, redes de datos, internet, entre otros.
SI	Soportes de Información	En esta categoría están: discos virtuales y físicos, memorias USB, discos y cintas, material impreso, entre otros, que permiten almacenar información de forma permanente durante o al menos largos periodos de tiempo.

NOMENCLATURA	TIPO DE ACTIVO	DESCRIPCIÓN
AUX	Equipamiento auxiliar	En esta categoría están: fuentes de alimentación, generadores eléctricos, equipos de climatización, cableado eléctrico, mobiliario, entre otros.
L	Instalaciones	En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones. Edificio, vehículos, instalaciones de refuerzo, entre otros.
P	Personal	Incluye personal fijo, eventual, terceros, entre otros. También se debe identificar a los responsables y custodios de la información asociada al activo; esto es importante porque a través de la identificación se realizará una mejor valoración para resguardar la información. Los custodios podrían ser los mismos servidores públicos o en otros casos una persona ajena a la entidad o institución pública.

Fuente: Elaboración Propia con base en los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público.

En el punto 3.1.4. se encuentran identificados los activos de los cuales se detallan los objetivos institucionales involucrados, proceso involucrado con el activo, la descripción, el tipo, ubicación, unidad responsable, custodio, y la valoración.

3.1.3. VALORACIÓN DE ACTIVOS DE INFORMACIÓN

La valoración de activos de información del SENATEX tiene como objetivo asegurar que la información asociada a los mismos reciba niveles de protección adecuados, ya que en base a su valor y otras características particulares se requerirá implementar o mejorar controles de seguridad.

A continuación, se conceptualiza las propiedades de la información asociadas a activos para su valoración, también es conveniente mencionar que se tiene las preguntas respectivas para clarificar la valoración asociada a cada característica del activo de información.

Tabla 2. PROPIEDADES DE LA INFORMACIÓN ASOCIADA A LOS ACTIVOS DE INFORMACIÓN DEL SENATEX

CARACTERÍSTICA	DESCRIPCIÓN	PREGUNTA PARA VALORACIÓN
DISPONIBILIDAD	Si una amenaza afectase su disponibilidad con consecuencias graves para el normal desarrollo de las actividades	¿Qué importancia tendría que el activo no estuviera disponible?
INTEGRIDAD	Una valoración alta de esta propiedad se da por el grado de afectación (daño grave) causado por la alteración voluntaria o no intencionada de los datos.	¿Qué importancia tendría que la información asociada al activo fuera modificada sin control?

CARACTERÍSTICA	DESCRIPCIÓN	PREGUNTA PARA VALORACIÓN
CONFIDENCIALIDAD	Se da en función del grado de afectación que ocasionaría la revelación o divulgación de información a personas no autorizadas.	¿Qué importancia tendría que la información asociada fuera conocida por personas no autorizadas?

Fuente: Elaboración Propia con base en los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público.

3.1.4. MATRIZ DE INVENTARIO Y VALORACIÓN

A continuación, en las siguientes tablas, se muestran los activos de información del SENATEX identificados y clasificados con su respectiva valoración.

Tabla 3. IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DEL SENATEX

No	ACTIVO	DESCRIPCIÓN	TIPO	UBICACIÓN	UNIDAD RESPONSABLE	RESPONSABLE	CUSTODIO
1	Base de datos del ERP TIM	Base de datos del sistema informático TIM	Datos o Información	Servidor TIM AS/400, Planta Telas, Piso 2 - Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
2	Base de datos del egatron	Sistema informático para registro de tiempos de confección por ítem	Datos o Información	Servidor, Piso 5, Edificio Yanacachi- Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
3	Archivo Documental del SENATEX	Conjunto de todos los documentos físicos que se tiene en el área de archivo central.	Datos o Información	Planta de Telas, Barrio Petrolero, Piso 1- Seguridad Alta	UAF	Jefe de la Unidad de Administración y Finanzas	Área de Archivo
4	Correo electrónico	Sistema web, para el uso del correo institucional @senatex.gob.bo	Servicios	Sistema informático web- Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
5	ERP TIM	Sistema Informático ERP especializado para la industria Textil, propiedad de Datatex. En su versión más moderna es conocida como NOW	Software – Aplicaciones informáticas	Servidor TIM AS/400, Planta Telas, Piso 2- Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
6	Sistema de	Sistema informático para la	Software –	Servidor, Piso 5,	UGST	Jefe de la Unidad	Área de

No	ACTIVO	DESCRIPCIÓN	TIPO	UBICACIÓN	UNIDAD RESPONSABLE	RESPONSABLE	CUSTODIO
	Ventas	gestión del inventario de almacenes de prendas de vestir y el sistema de punto de venta de tiendas	Aplicaciones informáticas	Edificio Yanacachi-Seguridad Alta		de Gestión de Servicios Técnicos	Sistemas
7	CODICE	Sistema informático para la gestión de la correspondencia interna y externa	Software – Aplicaciones informáticas	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
8	Zimbra	Correo electrónico Institucional	Servicios	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
9	Portal Web	Pagina institucional Publica contenido Normativo, Institucional	Servicios	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
10	WARA II	Sistema informático para la gestión de Plan Operativo Anual (POA)	Software – Aplicaciones informáticas	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
11	Servidor TIM AS/400	Servidor el sistema informático TIM	Hardware – Equipamiento informático	Planta de Telas, Barrio Petrolero-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas

SENATEX V° B° UGST. LORENZO ROGER FERRUFINO ROJAS

SENATEX V° B° TECNICO SOPORTE DE SISTEMAS

SENATEX V° B° UGST. PROFESIONAL EN ORGANIZACION ADMINISTRATIVA

HECHO EN BOLIVIA

No	ACTIVO	DESCRIPCIÓN	TIPO	UBICACIÓN	UNIDAD RESPONSABLE	RESPONSABLE	CUSTODIO
12	Servidor DELL R720	Vmware Servicio CODICE, Servicio de Correos	Hardware – Equipamiento informático	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
13	Servidor CISCO	Servidor DNS interno servidor, DNS Externo	Hardware – Equipamiento informático	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
14	Servidor DELL R710	Servicio Directorio Activo	Hardware – Equipamiento informático	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
15	Firewall Fortinet	Firewall, Enrutador, Servicio de DHCP	Redes de comunicaciones	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
16	New Sacha	Servicio de Archivos compartidos en la intranet	Soportes de información	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
17	Cintas de respaldo del TIM	Unidad de Almacenamiento servidor IBM TIM	Soportes de información	Planta de Telas, Barrio Petrolero-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas

SENATEX V°B° A.A.C.I.
SENATEX V°B° D.R.S.S.

HECHO EN BOLIVIA

No	ACTIVO	DESCRIPCIÓN	TIPO	UBICACIÓN	UNIDAD RESPONSABLE	RESPONSABLE	CUSTODIO
18	Sistema de aire acondicionado (2)	Permite establecer las condiciones de trabajo en el centro de datos	Equipamiento auxiliar	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
19	UPS	Unidad de Respaldo de Energía permite la continuidad de trabajo en caídas de tención.	Equipamiento auxiliar	Servidor, Piso 5, Edificio Yanacachi-Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
20	Equipos de Escritorio	Equipos de todas las dependencias del SENATEX	Hardware – Equipamiento informático	Planta de Hilandería, Planta de Telas, Unidad Central- seguridad Media	Todas las Unidades	Jefe/Responsable de Unidad	Jefe/Responsable de Unidad
21	Impresoras	Impresoras de Todas las dependencias del SENATEX	Hardware – Equipamiento informático	Planta de Hilandería, Planta de Telas, Unidad Central-Seguridad Media	Todas las Unidades	Jefe/Responsable de Unidad	Jefe/Responsable de Unidad
22	Telefonía	Central Telefónica y Terminales	Hardware – Equipamiento informático	Planta de Hilandería, Planta de Telas, Unidad Central- seguridad Media	Todas las Unidades	Jefe/Responsable de Unidad	Jefe/Responsable de Unidad
23	hubs	Equipo encargado de Vincular las redes	Hardware – Equipamiento informático	Planta de Hilandería, Planta de Telas, Unidad Central- Seguridad Alta	Todas las Unidades	Jefe/Responsable de Unidad	Jefe/Responsable de Unidad

SENATEX V°B° S.T.
SENATEX V°B° A.N.C.I. TECNICO SOPORTE DE SISTEMAS
SENATEX V°B° R.R.S. RESPONSABLE DE ORGANIZACION ADMINISTRATIVA

HECHO EN BOLIVIA

No	ACTIVO	DESCRIPCIÓN	TIPO	UBICACIÓN	UNIDAD RESPONSABLE	RESPONSABLE	CUSTODIO
24	Internet	Internet Fibra AXES - Entel Fibra	Redes de comunicaciones	Planta de Hilandería, Planta de Telas, Unidad Central- Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
25	Enlaces de Fibra Oscura	Enlaces de VPN por Fibra Óptica	Redes de comunicaciones	Planta de Hilandería, Planta de Telas, Unidad Central- Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
26	Biométricos	Registro de Asistencia del personal	Hardware – Equipamiento informático	Planta de Hilandería, Planta de Telas, Unidad Central- Seguridad Alta	UAF	Jefe de la Unidad de Administración y Finanzas	Área de Recursos Humanos
27	Circuito de vigilancia	Cámaras - Gavador DVR	Hardware – Equipamiento informático	Planta de Hilandería, Planta de Telas, Unidad Central- Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
28	Clave Criptográfica - Firma Digital	Método de autenticación electrónica	Claves criptográficas	Servidor, Piso 5, Edificio Yanacachi- Seguridad Alta	UAF	Jefe de la Unidad de Administración y Finanzas	Área Financiera
29	Active Directory	Servicio de autentificación para equipos y personal	Software – Aplicaciones informáticas	Servidor, Piso 5, Edificio Yanacachi- Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas

No	ACTIVO	DESCRIPCIÓN	TIPO	UBICACIÓN	UNIDAD RESPONSABLE	RESPONSABLE	CUSTODIO
30	Router	Dispositivos de conexión Inalámbrica	Hardware – Equipamiento informático	Planta de Hilandería, Planta de Telas, Unidad Central- Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
31	Swichs	Dispositivos de conexión de Redes de Datos	Redes de comunicaciones	Planta de Hilandería, Planta de Telas, Unidad Central- Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas
32	Planta Telas	Planta de Tejeduría del SENATEX	Instalaciones	Servidor, Piso 5, Edificio Yanacachi- Seguridad Alta	UAF	Jefe de la Unidad de Administración y Finanzas	Área de Activos
33	Personal Eventual	Personal encargado de Administrar y realizar mantenimiento preventivo y correctivo	Personal	Planta de Telas, Barrio Petrolero- Seguridad media	UAF	Jefe de la Unidad de Administración y Finanzas	Área de Recursos Humanos
34	Unidades Externas de Respaldo de Información	Unidades externas USB de respaldo de Información	Hardware – Equipamiento informático	Servidor, Piso 5, Edificio Yanacachi - Seguridad Alta	UGST	Jefe de la Unidad de Gestión de Servicios Técnicos	Área de Sistemas

Fuente: Elaboración Propia.

Tabla 4.VALORACIÓN DE ACTIVOS DE INFORMACIÓN

NO	ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	CRITICIDAD CUANTITATIVO	VALORACIÓN FINAL
1	Base de datos del ERP TIM	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
2	Base de datos del egatron	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
3	Archivo Documental del SENATEX	MUY ALTO	MUY ALTO	ALTO	5	MUY ALTO
4	Correo electrónico	MUY ALTO	MEDIO	MUY ALTO	4	ALTO
5	ERP TIM	MUY ALTO	ALTO	ALTO	4	ALTO
6	Sistema de Ventas	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
7	CODICE	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
8	Zimbra	ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
9	Portal Web	ALTO	MUY ALTO	MEDIO	4	ALTO
10	WARA II	MUY ALTO	MUY ALTO	ALTO	5	MUY ALTO
11	Servidor TIM AS/400	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
12	Servidor DELL R720	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
13	Servidor CISCO	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
14	Servidor DELL R710	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
15	Firewall Fortinet	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
16	New Sacha	ALTO	ALTO	MEDIO	4	ALTO

NO	ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	CRITICIDAD CUANTITATIVO	VALORACIÓN FINAL
17	Cintas de respaldo del TIM	MUY ALTO	ALTO	ALTO	4	ALTO
18	Sistema de aire acondicionado (2)	MEDIO	MEDIO	MEDIO	3	MEDIO
19	UPS	ALTO	ALTO	ALTO	4	ALTO
20	Equipos de Escritorio	ALTO	ALTO	ALTO	4	ALTO
21	Impresoras	MEDIO	MEDIO	MEDIO	3	MEDIO
22	Telefonía	MEDIO	MEDIO	BAJO	3	MEDIO
23	hubs	ALTO	ALTO	ALTO	4	ALTO
24	Internet	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
25	Enlaces de Fibra Oscura	ALTO	ALTO	MUY ALTO	4	ALTO
26	Biométricos	MEDIO	ALTO	ALTO	4	ALTO
27	Circuito de vigilancia	MUY ALTO	ALTO	MUY ALTO	5	MUY ALTO
28	Clave Criptográfica - Firma Digital	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
29	Active Directory	ALTO	ALTO	ALTO	4	ALTO
30	Router	ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO
31	Swichs	MUY ALTO	ALTO	ALTO	4	ALTO
32	Planta Telas	MUY ALTO	ALTO	MUY ALTO	5	MUY ALTO
33	Personal Eventual	ALTO	ALTO	ALTO	4	ALTO

NO	ACTIVO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	CRITICIDAD CUANTITATIVO	VALORACIÓN FINAL
34	Unidades Externas de Respaldo de Información	MUY ALTO	MUY ALTO	MUY ALTO	5	MUY ALTO

3.1.5. EVALUACIÓN DEL RIESGO

La evaluación del riesgo del SENATEX permitirá identificar las debilidades en cuanto a controles de seguridad inexistentes o ineficaces. Se sugiere que la evaluación se realice por tipo de activo agrupado por similares características.

La evaluación de riesgos es el proceso que permite determinar y categorizar las amenazas potenciales y vulnerabilidades asociadas a activos de información. El resultado de este proceso permitirá determinar la identificación de controles que reducirán los riesgos.

Para establecer el nivel de riesgo que cada amenaza con lleva al activo de información, en la siguiente tabla se muestran los criterios calificativos y los valores numéricos a ser utilizados para la valoración de la probabilidad de amenazas que podrían explorar alguna vulnerabilidad existente.

Para determinar la ocurrencia de la amenaza se responderá a las siguientes preguntas: i) ¿Ya ha sucedido antes?, ii) ¿Pasa muy seguido? y iii) ¿Podría suceder?

Para la valoración del riesgo se realizará el análisis de probabilidad de ocurrencia de las amenazas detectadas y el impacto que estas tendrán dentro de los procesos de la institución.

Tabla 5. CRITERIOS DE VALORACIÓN CUALITATIVA DE RIESGO

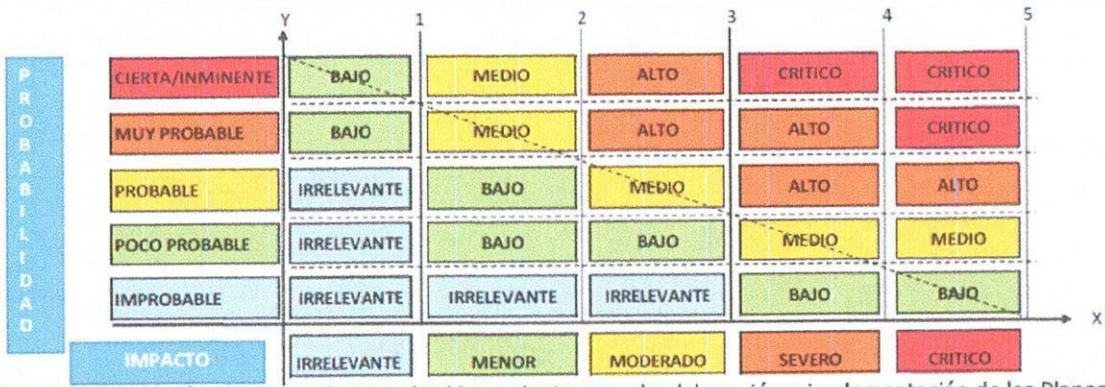
NIVEL	PROBABILIDAD	IMPACTO
5	Cierta/Inminente	Critico
4	Muy Probable	Severo

NIVEL	PROBABILIDAD	IMPACTO
3	Probable	Moderado
2	Poco Probable	Menor
1	Improbable	Irrelevante

Fuente: Elaboración Propia con base en los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público.

A continuación, se presenta la matriz de valoración del riesgo cualitativo.

Gráfico 1. MATRIZ DE VALORACIÓN DE RIESGO CUALITATIVO



Fuente: Elaboración Propia con base en los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público.

A continuación, se presenta las tablas respectivas de la valoración de riesgos de los diferentes activos de información.

Tabla 6. EVALUACIÓN DEL RIESGO

No	ACTIVO	AMENAZA	SITUACIÓN	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
1	Sistemas de Información	Ataques de malware	Cuando se propague malware (virus, troyanos o ransomware)	Defectos conocidos en el software	CIERTA/ INMINENTE	SEVERO	CRÍTICO
		Inyección de código	Cuando se manipule datos o se ejecute acciones no autorizadas.	Defectos conocidos en el software	PROBABLE	SEVERO	ALTO
		Acceso no autorizado o Suplantación de identidad	Cuando un usuario abandona una estación de trabajo sin cerrar la sesión, alguien más podría acceder a la información y recursos disponibles en esa sesión activa.	Ausencia de terminación de la sesión cuando se abandona la estación de trabajo	PROBABLE	MODERADO	MEDIO
		Fugas de información	Cuando un usuario recibe derechos de acceso que exceden sus responsabilidades o nivel de autorización.	Asignación errada de los derechos de acceso	POCO PROBABLE	MODERADO	BAJO
		Errores humanos	Cuando se malinterprete la navegación y se cometa errores de entrada de datos o seleccionar opciones incorrectas	Interfaz de usuario compleja	POCO PROBABLE	MENOR	BAJO
		Dificultad en el mantenimiento y la gestión	Ausencia de documentación dificulta la comprensión de la estructura y el funcionamiento de los sistemas de información	Ausencia de documentación	PROBABLE	MENOR	BAJO

No	ACTIVO	AMENAZA	SITUACIÓN	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
		Desarrollo defectuoso o incorrecto	Cuando no se tienen especificaciones claras, podrían interpretar mal los requisitos del sistema	Especificaciones incompletas o no claras para los desarrolladores	POCO PROBABLE	MENOR	BAJO
		Pérdida de datos críticos	Cuando exista fallo del sistema, corrupción de datos, ataque cibernético, o desastres naturales.	Ausencia de copias de respaldo	PROBABLE	SEVERO	ALTO
		Ataques de ransomware	Cuando los atacantes cifran los datos y exigen un rescate para su recuperación	Ausencia de copias de respaldo	POCO PROBABLE	CRÍTICO	MEDIO
2	Correo electrónico	Manipulación de la cuenta	Cuando un tercero malintencionado manipule la cuenta del usuario.	Ausencia de terminación de la sesión cuando se abandona la estación de trabajo	POCO PROBABLE	MODERADO	BAJO
		Fugas de información confidencial	Cuando los usuarios realizan copias no controladas de correos electrónicos que contienen información sensible o confidencial.	Copia no controlada	PROBABLE	SEVERO	ALTO
		Phishing	Cuando los correos electrónicos o mensajes aparentan ser de fuentes legítimas y no exista autenticación.	Ausencia de identificación y autentificación de emisor y receptor	MUY PROBABLE	SEVERO	ALTO
3	Portal Web	Inyección de código malicioso	Cuando los atacantes acceden, modifican o eliminan datos.	Configuración incorrecta de parámetros	PROBABLE	SEVERO	ALTO

No	ACTIVO	AMENAZA	SITUACIÓN	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
		Exposición de información sensible	Cuando los permisos de directorios no se establecen correctamente.	Configuración incorrecta de parámetros	PROBABLE	MODERADO	MEDIO
		Inconsistencias en la configuración	Cuando existan configuraciones de permisos incorrectos o inconsistencias entre versiones del software.	Ausencia de control de cambios eficaz	POCO PROBABLE	SEVERO	MEDIO
4	Clave Criptográfica - Firma Digital	Falta de cifrado de extremo a extremo	Cuando se utiliza un método de transmisión de datos inadecuado	Transferencia de contraseñas en claro	POCO PROBABLE	SEVERO	MEDIO
		Almacenamiento inseguro	Cuando la contraseña se almacena en bases de datos o sistemas que carecen de medidas de seguridad adecuadas	Ser accesible para personas no autorizadas	PROBABLE	CRÍTICO	ALTO
5	Unidades de Respaldo	Fallas en el blindaje	Cuando existe interferencia generada por dispositivos como antenas, motores, transformadores u otros dispositivos eléctricos de alta potencia..	Sensibilidad a la radiación electromagnética	POCO PROBABLE	CRÍTICO	MEDIO
		Copias no autorizadas y/o Distribución no controlada	Cuando el personal copia datos a un dispositivo externo y/o lo distribuye a destinatarios no autorizados.	La información puede caer en manos equivocadas o ser utilizados incorrectamente	IMPROBABLE	CRÍTICO	BAJO
		Acceso no regulado	Cuando las copias de seguridad no están controladas adecuadamente en términos de acceso.	Personas no autorizadas puedan ver, modificar o eliminar datos críticos.	IMPROBABLE	CRÍTICO	BAJO

No	ACTIVO	AMENAZA	SITUACIÓN	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
6	Base de datos	Copia de seguridad no asegurada	Cuando las copias de seguridad de la base de datos no están encriptadas o protegidas adecuadamente.	Acceso a información sensible	IMPROBABLE	CRÍTICO	BAJO
		Permisos incorrectos	Cuando se configura permisos excesivos a ciertos usuarios o se permite el acceso a partes sensibles de la base de datos.	Configuración incorrecta de parámetros	PROBABLE	CRÍTICO	ALTO
7	Firewall	Conexiones no seguras entre zonas de red	Cuando no está implementado o configurado adecuadamente	Arquitectura insegura de la red o ubicación inapropiada del firewall	MUY PROBABLE	CRÍTICO	CRÍTICO
		Configuraciones incorrectas	Cuando las reglas de firewall tengan una configuración errónea.	Configuración incorrecta de parámetros	MUY PROBABLE	CRÍTICO	CRÍTICO
		Ataques de envenenamiento de caché o redireccionamiento de tráfico	Cuando existe una mala gestión en la tolerancia a fallos en el enrutamiento	Gestión inadecuada de la red (Tolerancia a fallos en el enrutamiento)	PROBABLE	CRÍTICO	ALTO
8	Dispositivos de Conexión de redes	Intercepción de datos sensibles	Cuando los cables, conexiones inalámbricas, transmisiones de datos, etc., no están debidamente protegidas.	Líneas de comunicación sin protección	MUY PROBABLE	MODERADO	ALTO
		Pérdida de rendimiento de red	Cuando existe lentitud en la red o interrupciones en la comunicación	Conexión deficiente de los cables	POCO PROBABLE	MODERADO	BAJO

No	ACTIVO	AMENAZA	SITUACIÓN	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
9	Conectividad Internet	Cambios no autorizados en la configuración de red	Cuando existe apertura de puertos innecesarios o configuraciones que debilitan la seguridad.	Ausencia de control de cambios eficaz	POCO PROBABLE	SEVERO	MEDIO
		Escasez de defensas perimetrales	Cuando no existe defensas perimetrales sólidas, como firewalls, IDS/IPS (Sistemas de Detección/Prevención de Intrusiones) o sistemas de filtrado	Arquitectura insegura de la red	POCO PROBABLE	SEVERO	MEDIO
10	Sistema de aire acondicionado	Cortocircuitos o fallas eléctricas	Cuando existe variaciones extremas de temperatura	Susceptibilidad a las variaciones de temperatura	POCO PROBABLE	SEVERO	MEDIO
11	UPS	Riesgo de fallas	Cuando existe variaciones extremas de temperatura	Daños internos en los componentes electrónicos	IMPROBABLE	SEVERO	BAJO
		Fallos o daños en la batería	Cuando existen sobrecargas, fluctuaciones extremas de temperatura o defectos inherentes	Incapacidad del UPS para proporcionar energía durante un corte	POCO PROBABLE	SEVERO	MEDIO
12	Servidores	Fallos en sistemas de refrigeración	Cuando existe variaciones extremas de temperatura	Susceptibilidad a las variaciones de temperatura	POCO PROBABLE	MODERADO	BAJO
		Ataques cibernéticos	Cuando los atacantes bloquean o eliminan datos críticos	Ausencia de copias de respaldo	PROBABLE	CRÍTICO	ALTO
13	Archivo Documental del SENATEX	Transferencia de responsabilidad o cambio de personal	Cuando ocurre un cambio o transferencia de personal	Ausencia de documentación o manejo inapropiado	POCO PROBABLE	MODERADO	BAJO

No	ACTIVO	AMENAZA	SITUACIÓN	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
		Desastres naturales o físicos	Cuando ocurra incendios, inundaciones, terremotos o incluso robos	Ausencia de copias de respaldo	IMPROBABLE	CRÍTICO	BAJO
14	Personal Eventual	Filtración de Información o Violaciones de cumplimiento	Cuando el personal podría compartir información confidencial a través de canales inseguros o no autorizados	Ausencia de políticas para el uso de los medios de telecomunicaciones y mensajería	PROBABLE	SEVERO	ALTO
		Ataques de phishing	Cuando se puede revelar información personal a través de correos electrónicos falsos, mensajes o llamadas.	Falta de conciencia acerca de la seguridad	POCO PROBABLE	SEVERO	MEDIO
15	Equipos de Escritorio	Mantenimiento inadecuado	Cuando no existe limpieza y mantenimiento adecuado.	Susceptibilidad a la humedad, el polvo y la suciedad.	POCO PROBABLE	MODERADO	BAJO
		Ambientes no controlados	Cuando se utiliza en planta los equipos de escritorio pueden estar expuestos a niveles de humedad o contaminantes.	Susceptibilidad a la humedad, el polvo y la suciedad.	POCO PROBABLE	MENOR	BAJO
16	Impresoras	Falla fisica de componentes o Alteración del funcionamiento	Cuando existen cambios no autorizados.	Ausencia de un eficiente control de cambios en la configuración	POCO PROBABLE	IRRELEVANTE	IRRELEVANTE
17	Control de Ingresos	Ingreso no autorizado	Cuando se asignan derechos de acceso de manera incorrecta, individuos no autorizados podrían obtener acceso a	Asignación errada de los derechos de acceso	PROBABLE	MODERADO	MEDIO

No	ACTIVO	AMENAZA	SITUACIÓN	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
			información confidencial.				
18	Instalaciones	Ingreso no autorizado	Cuando el control de acceso físico es inadecuado.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones o recintos	PROBABLE	MODERADO	MEDIO

Fuente: Elaboración Propia.

3.1.6. TRATAMIENTO DE RIESGO

El tratamiento del riesgo implica tomar decisiones, a continuación, se detallará el tratamiento a considerar.

Tabla 7. TRATAMIENTO DEL RIESGO

TRATAMIENTO	DESCRIPCIÓN
ACEPTAR	No será necesario la aplicación de o implementación de controles, estos riesgos serán aceptados teniendo en cuenta que existe la posibilidad de ocurrencia del mismo sin tomar medidas de acción ni control.
REDUCIR	Implementación de un control de seguridad de la información que ofrezca mayores beneficios Implica la aplicación de los controles descritos en la "MATRIZ DE CONTROLES IMPLEMENTADOS Y POR IMPLEMENTAR", para reducir el riesgo del activo de información de la institución.

TRATAMIENTO	DESCRIPCIÓN
EVITAR	O eliminación del riesgo, lo que conllevaría realizar el análisis de eliminación del activo de información para eliminar el riesgo. Este tratamiento deberá ser justificado y documentado en caso de implementarlo.
TRANSFERIR	Involucra la acción de un tercero para poder mitigar el riesgo, lo no implicaría que se transfieran responsabilidades, por lo cual se deberá realizar seguimiento del riesgo trasferido para asegurar su tratamiento.

3.1.6.1. CRITERIOS PARA LA ACEPTACIÓN DEL RIESGO

Se ha considerado que los riesgos identificados como "CRITICO O ALTO" al término de la actividad de Evaluación de Riesgos podrán ser aceptados sin requerir de un tratamiento, solo bajo las siguientes condiciones:

- ✓ El costo de tratar el riesgo se estima como mayor a la pérdida o impacto económico generado por la ocurrencia del mismo.
- ✓ El costo de implementar el control o controles esta fuera de presupuesto del año en curso.

3.1.7. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN PARA EL TRATAMIENTO DE LOS RIESGOS

En el marco de la Gestión de Seguridad de la Información y de los recursos humanos el SENATEX dispone:

CONTROL 1. SEGURIDAD EN RECURSOS HUMANOS

a. **Control de Acceso:** Implementar sistemas de gestión de acceso que regulen quién tiene acceso a qué información. Esto incluye el uso de contraseñas seguras, autenticación de múltiples factores y la asignación de permisos según roles y responsabilidades.

   Asimismo, toda vez que se produzca la desvinculación del personal eventual, consultor o cualquiera que tenga un vínculo laboral con el SENATEX, se deben cancelar o dar de baja los derechos de acceso a los sistemas de información y servicios tecnológicos.

b. **Formación y Concienciación:** Capacitar al personal en buenas prácticas de seguridad, concienciándolos sobre la importancia de proteger la información confidencial, detectar intentos de fraude (phishing) y manejar adecuadamente la información.

c. **Control de Dispositivos:** Establecer políticas de uso para dispositivos móviles y restringir el acceso a la información confidencial desde dispositivos no autorizados. El cifrado de datos en dispositivos móviles y la implementación de herramientas de control remoto también son importantes.

d. **Actualización y Mantenimiento de Sistemas:** Mantener actualizados todos los sistemas informáticos, aplicar parches de seguridad y utilizar software actualizado con medidas de seguridad para proteger la información contra vulnerabilidades conocidas.

e. **Acuerdo de Confidencialidad:** Se deberá analizar la pertinencia de implementar el mismo como documento separado o incorporarlo en el contrato de relación laboral (cuando corresponda), con la finalidad de contar con un compromiso de confidencialidad deberá respetar los datos de carácter personal, garantizar la privacidad y protección de la información personal identificable.

CONTROL 2. GESTIÓN DE ACTIVOS DE INFORMACIÓN

a. **Inventario de Activos de Información:** Mantener un inventario actualizado de todos los activos de información es esencial. Esto implica identificar y catalogar todos los recursos críticos, como bases de datos, servidores, documentos, aplicaciones, dispositivos, y asignarles etiquetas de clasificación según su importancia y nivel de seguridad.

b. **Clasificación y Etiquetado de Información:** Definir un sistema de clasificación que determine la sensibilidad de la información. Esto puede incluir etiquetas o niveles de clasificación (público, interno, confidencial) para asegurar que se apliquen los controles de seguridad adecuados.

c. **Protección de Activos Físicos:** Implementar medidas de seguridad física para proteger los activos de información. Esto implica restringir el acceso a salas de servidores, archivadores o cualquier lugar donde se almacenen activos físicos sensibles, utilizando cámaras de vigilancia, sistemas de acceso con tarjetas, cerraduras de seguridad, etc.

d. **Gestión de Versiones y Actualizaciones:** Controlar las versiones de software, hardware y documentación para asegurarse de que estén actualizadas y se cumplan las políticas de seguridad. Esto implica aplicar parches de seguridad, actualizaciones y revisiones en tiempo y forma.

e. **Copias de Seguridad y Recuperación:** Realizar copias de seguridad periódicas de los activos críticos y tener un plan de recuperación ante desastres. Estas medidas garantizan la disponibilidad de la información en caso de fallos o eventos catastróficos.

f. **Retiro Seguro de Activos:** Al retirar activos de información, ya sea hardware obsoleto o documentos confidenciales, es esencial garantizar su eliminación segura. Esto puede implicar el borrado seguro de discos duros, la destrucción de documentos sensibles y la eliminación de cualquier dato personal o confidencial.

CONTROL 3. CONTROL DE ACCESOS

a. **Políticas de Acceso:** Establecer políticas claras que definen quién tiene acceso a qué recursos, asimismo, reglas que determinan los niveles de acceso y las circunstancias bajo las cuales se otorgan o revocan los permisos.

b. **Gestión de Identidad:** Para la gestión de Usuarios se debe considerar la creación, modificación y eliminación de cuentas de usuario. Por otra parte, para el control de la asignación de Privilegios debe ser según las responsabilidades del usuario.

CONTROL 4. CRIPTOGRAFÍA

a. **Protocolos de Seguridad:** SSL/TLS (Secure Socket Layer/Transport Layer Security): Protocolos que proporcionan comunicaciones seguras a través de internet mediante la encriptación de datos.

b. **Gestión de Claves:** Implementación de políticas y procedimientos para administrar las claves de encriptación, incluyendo su generación, almacenamiento, distribución, rotación y eliminación segura.

CONTROL 5. SEGURIDAD FÍSICA Y AMBIENTAL

a. **Protección de Equipos e Instalaciones:** Resguardo de Hardware: Mantener servidores, dispositivos de almacenamiento y otros equipos críticos en áreas seguras y protegidas.

b. **Sistemas de Alarma:** Instalación de sistemas de alarma para detectar intrusiones, incendios u otras emergencias.

c. **Protección contra Desastres y Elementos Ambientales:**

- **Control Ambiental:** Asegurarse de que las áreas de almacenamiento y servidores estén protegidas contra riesgos como incendios, inundaciones, temperatura inadecuada, etc.
- **Sistemas de Energía y Respaldo:** Implementar fuentes de energía alternativas, así como sistemas de respaldo, para garantizar la continuidad de las operaciones incluso en casos de cortes de energía.

d. **Controles de Seguridad Ambiental:**

- **Control de Ruido:** Reducción de ruidos y vibraciones que puedan afectar la integridad de sistemas de almacenamiento o procesamiento de datos.
- **Control de Polvo y Contaminantes:** Mantenimiento adecuado para evitar la acumulación de polvo y la exposición a contaminantes que puedan dañar equipos.

CONTROL 6. SEGURIDAD DE LAS OPERACIONES

a. **Gestión de Incidentes:**

- **Planes de Respuesta a Incidentes:** Desarrollo de procedimientos detallados para manejar incidentes de seguridad, incluyendo cómo responder a brechas de seguridad, ataques cibernéticos, o fallos de sistemas.
- **Equipo de Respuesta a Incidentes:** Designación de un equipo especializado para gestionar y responder a incidentes, minimizando así los impactos potenciales.

b. Mantenimiento de Sistemas y Actualizaciones:

- **Programas de Mantenimiento Preventivo:** Implementación de mantenimiento regular y actualizaciones de software y hardware para reducir vulnerabilidades.
- **Aplicación de Parches de Seguridad:** Actualización de sistemas y aplicaciones con los últimos parches de seguridad para mitigar riesgos de explotación.

c. Gestión de Configuración:

- **Gestión de Configuración de Software y Hardware:** Documentación y seguimiento de la configuración de sistemas para garantizar que cumplan con las políticas de seguridad.
- **Control de Versiones y Cambios:** Administración y seguimiento de versiones de software y hardware para mantener la integridad y la compatibilidad.

CONTROL 7. SEGURIDAD DE LAS COMUNICACIONES

a. Encriptación de Comunicaciones:

- **Uso de Protocolos Seguros:** Implementación de protocolos como SSL/TLS en la comunicación web para cifrar los datos en tránsito.
- **VPN (Red Privada Virtual):** Utilización de conexiones VPN para encriptar el tráfico entre ubicaciones remotas y la red central.

b. Control de Acceso y Autenticación:

- **Autenticación Fuerte:** Requerir autenticación multifactorial para acceder a sistemas o datos sensibles.
- **Control de Acceso a Redes y Segmentación:** Establecimiento de zonas seguras y restricción de acceso a ciertas áreas de la red.

c. Protección contra Amenazas Externas:

- **Firewalls y Sistemas de Detección y Prevención de Intrusos:** Implementación de sistemas para detectar y bloquear intentos de intrusión desde fuentes externas.
- **Filtrado de Contenido Web:** Uso de filtros para bloquear sitios web maliciosos o no autorizados.

d. Seguridad de Correo Electrónico:

- **Filtrado de Correo no Deseado (SPAM):** Implementación de sistemas para filtrar y bloquear correos no deseados.
- **Cifrado de Correo Electrónico:** Utilización de cifrado para proteger la confidencialidad de los mensajes.

CONTROL 8. DESARROLLO, MANTENIMIENTO Y ADQUISICIÓN DE SISTEMAS

a. Gestión de Parches y Actualizaciones:

- **Plan de Gestión de Parches:** Establecimiento de un plan para aplicar parches y actualizaciones críticas de seguridad de manera oportuna.
- **Pruebas Post-Actualización:** Verificación de la estabilidad y seguridad de los sistemas después de aplicar parches o actualizaciones.

b. Control de Versiones y Configuraciones:

- **Control de Versiones:** Gestión de versiones para garantizar que solo las versiones aprobadas estén en uso.
- **Gestión de Configuraciones:** Documentación y seguimiento de configuraciones para mantener la integridad y seguridad de los sistemas.

c. Adquisición de Software y Equipamiento Seguro:

- **Evaluación de Proveedores:** Revisión de la seguridad de los proveedores de software o equipos para garantizar que cumplan con estándares de seguridad.
- **Pruebas de Seguridad de Equipamiento y Software:** Realización de pruebas de seguridad antes de la adquisición para identificar posibles riesgos.

CONTROL 9. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

a. Plan de Respuesta a Incidentes:

- **Desarrollo de Planes:** Creación de un plan formal de respuesta a incidentes que describa los procedimientos a seguir cuando ocurren eventos de seguridad.

b. Equipo de Respuesta a Incidentes (CSIRT):

- **Designación de Equipo:** Establecimiento de un equipo dedicado para responder a incidentes, con roles y responsabilidades claramente definidos.

- **Entrenamiento del Equipo:** Capacitación periódica para que el equipo esté preparado y actualizado sobre las últimas amenazas y respuestas.

c. Contención, Erradicación y Recuperación:

- **Contención de Incidentes:** Acciones inmediatas para contener y prevenir la propagación del incidente.
- **Erradicación de la Amenaza:** Eliminación de la amenaza y restablecimiento de la normalidad en los sistemas afectados.
- **Recuperación de Datos:** Restauración de datos y sistemas afectados a un estado seguro.

CONTROL 10. PLAN DE CONTINGENCIAS TECNOLÓGICAS

a. Desarrollo de Estrategias de Contingencia:

- Establecimiento de un marco que describa cómo responder a diferentes tipos de incidentes.
- Creación de planes específicos para la recuperación de sistemas críticos y datos importantes.

b. Respaldo y Recuperación de Datos:

- Implementación de rutinas de copias de seguridad regulares para asegurar la disponibilidad y protección de los datos.
- Desarrollo de un plan detallado de recuperación en caso de pérdida de datos o fallas del sistema.

c. Pruebas y Ejercicios de Simulacro:

- Realización de simulacros y pruebas regulares para evaluar la efectividad y eficacia del plan de contingencias.
- Identificación de áreas de mejora a través de estos ejercicios.

d. Gestión de Proveedores y Contratos:

- Revisión y aseguramiento de que los proveedores de servicios tengan planes de contingencia y respaldo.
- Inclusión de cláusulas en los contratos que regulen la continuidad del servicio en situaciones de emergencia.

3.1.8. MATRIZ DE CONTROLES IMPLEMENTADOS Y POR IMPLEMENTAR

VALORACIÓN DE RIESGOS			TRATAMIENTO		
#	Activo	Amenaza	Nivel de Riesgo	Control Existente	Control Recomendado (PISI 3.1.7)
1	Sistemas de Información	Ataques de malware	CRÍTICO	EXISTENTE	**Control 7, Inciso B**
		Inyección de código	ALTO	EXISTENTE	**Control 6, Inciso A**
		Acceso no autorizado o Suplantación de identidad	MEDIO	EXISTENTE	**Control 3, Inciso A e Inciso B**
		Fugas de información	BAJO	EXISTENTE	**Control 7, Inciso D y Control 1, Inciso A**
		Errores humanos	BAJO	EXISTENTE	**Control 1, Inciso B**
		Dificultad en el mantenimiento y la gestión	BAJO	INEXISTENTE	**Control 6, Inciso B e Inciso C**
		Desarrollo defectuoso o incorrecto	BAJO	INEXISTENTE	**Control 8, Inciso A**
		Pérdida de datos críticos	ALTO	(*) INEXISTENTE	**Control 10, Inciso B**
2	Correo electrónico	Manipulación de la cuenta	BAJO	EXISTENTE	**Control 6, Inciso**

VALORACIÓN DE RIESGOS			TRATAMIENTO		
#	Activo	Amenaza	Nivel de Riesgo	Control Existente	Control Recomendado (PISI 3.1.7)
		Fugas de información confidencial	ALTO	EXISTENTE	**Control 7, Inciso D**
		Phishing	ALTO	EXISTENTE	**Control 7, Inciso D**
3	Portal Web	Inyección de código malicioso	ALTO	INEXISTENTE	**Control 6, Inciso A**
		Exposición de información sensible	MEDIO	EXISTENTE	-
		Inconsistencias en la configuración	MEDIO	EXISTENTE	**Control 6, Inciso C**
4	Clave Criptografica - Firma Digital	Falta de cifrado de extremo a extremo	MEDIO	EXISTENTE	**Control 5, Inciso B**
		Almacenamiento inseguro	ALTO	EXISTENTE	**Control 5, Inciso B**
5	Unidades de Respaldo	Copias no autorizadas y/o Distribución no controlada	BAJO	EXISTENTE	**Control 10, Inciso B**
		Acceso no regulado	BAJO	(*) INEXISTENTE	**Control 3, Inciso A**
6	Base de datos	Copia de seguridad no asegurada	BAJO	(*) INEXISTENTE	**Control 8, Inciso A**

VALORACIÓN DE RIESGOS			TRATAMIENTO		
#	Activo	Amenaza	Nivel de Riesgo	Control Existente	Control Recomendado (PISI 3.1.7)
		Permisos incorrectos	ALTO	EXISTENTE	**Control 8, Inciso A**
7	Firewall	Conexiones no seguras entre zonas de red	BAJO	EXISTENTE	**Control 8, Inciso A**
		Configuraciones incorrectas	BAJO	EXISTENTE	**Control 8, Inciso B**
		Ataques de envenenamiento de caché o redireccionamiento de tráfico	MEDIO	EXISTENTE	**Control 6, Inciso A**
8	Dispositivos de Conexión de redes	Intercepción de datos sensibles	ALTO	(*) INEXISTENTE	**Control 3, Inciso A**
		Pérdida de rendimiento de red	BAJO	EXISTENTE	**Control 3, Inciso A**
9	Conectividad Internet	Cambios no autorizados en la configuración de red	MEDIO	(*) INEXISTENTE	**Control 3, Inciso A**
		Escasez de defensas perimetrales	MEDIO	EXISTENTE	**Control 8, Inciso A**
10	Sistema de aire acondicionado	Cortocircuitos o fallas eléctricas	MEDIO	(*) INEXISTENTE	**Control 6, Inciso A**

VALORACIÓN DE RIESGOS			TRATAMIENTO		
#	Activo	Amenaza	Nivel de Riesgo	Control Existente	Control Recomendado (PISI 3.1.7)
11	UPS	Riesgo de fallas	BAJO	(*) INEXISTENTE	**Control 6, Inciso A**
		Fallos o daños en la batería	MEDIO	(*) INEXISTENTE	**Control 6, Inciso A**
12	Servidores	Fallos en sistemas de refrigeración	BAJO	INEXISTENTE	**Control 6, Inciso B**
		Ataques cibernéticos	ALTO	(*) INEXISTENTE	**Control 6, Inciso A**
13	Archivo Documental del SENATEX	Transferencia de responsabilidad o cambio de personal	BAJO	(*) INEXISTENTE	**Control 1, Inciso A e Inciso E**
		Desastres naturales o físicos	BAJO	INEXISTENTE	**Control 2, Inciso E Control 5, Inciso C**
14	Personal Eventual	Filtración de Información o Violaciones de cumplimiento	ALTO	EXISTENTE	**Control 1, Inciso E**
		Ataques de phishing	MEDIO	EXISTENTE	**Control 1, Inciso C**
15	Equipos de Escritorio	Mantenimiento inadecuado	BAJO	EXISTENTE	**Control 5, Inciso C**
		Ambientes no controlados	BAJO	EXISTENTE	**Control 5, Inciso C**

VALORACIÓN DE RIESGOS			TRATAMIENTO		
#	Activo	Amenaza	Nivel de Riesgo	Control Existente	Control Recomendado (PISI 3.1.7)
16	Impresoras	Falla física de componentes o Alteración del funcionamiento	IRRELEVANTE	EXISTENTE	**Control 5, Inciso A**
17	Control de Ingresos	Ingreso no autorizado	MEDIO	EXISTENTE	**Control 3, Inciso B**
18	Instalaciones	Ingreso no autorizado	MEDIO	EXISTENTE	**Control 3, Inciso A**

(*) Para estos casos es importante mencionar que a la fecha se tomaron acciones pertinentes pero las mismas no se encuentran formalizadas, o en su defecto no se generó un respaldo documental.

CAPITULO IV
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4.1. INTRODUCCIÓN

La implementación de políticas de seguridad de la información constituye un elemento fundamental en la gestión efectiva de los riesgos asociados a la administración de datos en una organización. Estas políticas, en esencia, establecen un marco integral de controles diseñados para mitigar riesgos y salvaguardar la integridad, disponibilidad y confidencialidad de los activos de información.

En el contexto específico del Servicio Nacional Textil, la iniciativa de incorporar políticas de seguridad de la información busca fortalecer la resiliencia de la organización frente a posibles amenazas, sin interferir con las operaciones cotidianas del personal. Más bien, se propone optimizar la eficiencia de los procesos, asegurando al mismo tiempo la protección de la información sensible a través de la disponibilidad, integridad y confidencialidad de los activos de información.

Es crucial destacar que la efectividad de estas políticas no solo depende de la implementación técnica de controles, sino también de la internalización de los principios de seguridad en la cultura organizacional. Para lograr esto, es imperativo obtener un compromiso explícito por parte de todo el personal de la institución, quienes deben liderar la difusión y asegurar el cumplimiento de la presente Política de Seguridad. Este compromiso no solo fortalece la seguridad de la información, sino que también contribuye a forjar una cultura de conciencia y responsabilidad en todos los niveles de la organización.

4.2. TÉRMINOS Y DEFINICIONES

- **SENATEX:** Dirección del Servicio Nacional de Textil, es una institución con la misión de brindar servicio textil de calidad en toda Bolivia.
- **Activos de información:** Datos o información, software, hardware, servicios, personas o conocimiento asociados con el manejo de la información que tiene valor para la organización.
- **Autenticidad:** Propiedad de la información de ser genuina y ser capaz de ser verificada y de confianza; confianza en la validez de una transmisión, un mensaje, o remitente del mensaje.
- **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.
- ***Backup.*** – Una copia de seguridad, respaldo, copy backup, copia de respaldo, copia de reserva (del inglés backup) en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida

- **Comité de Seguridad de la Información (CSI):** Equipo de trabajo conformado para gestionar, promover e impulsar iniciativas en seguridad de la información.
- **Confidencialidad:** Propiedad por la cual la información no esté disponible o divulgada a individuos, entidades o procesos no autorizados.
- **Custodio del activo de información:** Servidor público encargado de administrar y hacer efectivo los controles de seguridad definidos por el responsable del activo de información.
- **Disponibilidad:** Propiedad por la cual se tiene acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.
- **Incidente:** Es la violación o amenaza que afectan la confidencialidad, disponibilidad y la integración como la continuidad de los servicios que son ofrecidos.
- **Integridad:** La propiedad de salvaguardar la exactitud, completitud de la información y los métodos de procesamiento.
- **Política de Seguridad de la Información (PSI):** Acciones o directrices que establecen la postura institucional en relación a la seguridad de la información, incluidas dentro del Plan Institucional de Seguridad de la Información.
- **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 en la entidad o institución pública.
- **Privilegios:** Son los roles que tiene asignado un usuario o sistema que le permiten realizar ciertas acciones sobre la información disponible.
- **Responsable de Seguridad de la Información (RSI):** Servidor público responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información.
- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y confiabilidad.
- **Seguridad informática:** Es el conjunto de normas, procedimientos y herramientas, las que se enfocan en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.
- **VPN:** Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.
- **Vulnerabilidad:** Debilidad del sistema informática que puede ser utilizada para causar algún tipo de daño.

4.3. OBJETIVO GENERAL

Establecer un marco integral de la Política de Seguridad de la Información (PSI) en el Servicio Nacional Textil, con el propósito de proteger y garantizar la disponibilidad, integridad y confidencialidad de los activos de información, por medio de la implementación, monitoreo y mejora continua de los controles y medidas que minimicen los riesgos asociados a la administración de datos, promoviendo una cultura organizacional consciente y comprometida con la seguridad de la información dentro de la Institución.

4.4. OBJETIVOS ESPECÍFICOS

La consecución de los siguientes objetivos contribuirá de manera significativa a la implementación exitosa de la Política de Seguridad de la Información (PSI) en el Servicio Nacional Textil, fortaleciendo la postura de la organización frente a posibles amenazas y promoviendo una gestión de la información más segura y eficiente.

i. Desarrollar un Conjunto de Políticas Adaptadas

- ✓ Definir políticas específicas que se ajusten a las características y necesidades particulares del Servicio Nacional Textil.
- ✓ Adaptar las políticas a las mejores prácticas y estándares de seguridad de la información reconocidos.

ii. Incorporar Controles Efectivos

- ✓ Identificar y establecer controles técnicos y procedimentales adecuados para mitigar los riesgos asociados a la gestión de la información.
- ✓ Garantizar la implementación efectiva de controles que salvaguarden la integridad, disponibilidad y confidencialidad de los activos de información.

iii. Optimizar la Eficiencia Operativa:

- ✓ Integrar las políticas de seguridad de la información en los procesos existentes sin interrupciones significativas en las operaciones diarias.
- ✓ Mejorar la eficiencia de los procedimientos mediante la aplicación de controles que no comprometan la productividad del personal.

iv. Fomentar la Conciencia y Compromiso Organizacional:

- ✓ Sensibilizar a todo el personal acerca de la importancia de la seguridad de la información.
- ✓ Facilitar la participación activa y el compromiso de los colaboradores mediante la promoción de prácticas seguras en el manejo de la información.

v. Integrar Principios de Seguridad en la Cultura Organizacional:

- ✓ Obtener un compromiso manifiesto de las máximas autoridades y líderes de las unidades para asegurar la difusión y cumplimiento de la política de seguridad.

- ✓ Fomentar la internalización de los principios de seguridad en la cultura organizacional a través de programas de capacitación y comunicación efectiva.

4.5. ALCANCE

Las políticas de seguridad de la información del Servicio Nacional Textil abarcarán de manera integral todas las áreas y procesos que involucren la gestión, manipulación y resguardo de información sensible. Este alcance incluye, pero no se limita a:

a. Activos de Información:

- Identificación y clasificación de los activos de información críticos para la operación y la toma de decisiones en la organización.
- Establecimiento de medidas específicas para garantizar la disponibilidad, integridad y confidencialidad de estos activos.

b. Procesos Operativos:

- Integración de controles de seguridad en los procesos operativos existentes, asegurando la continuidad de las operaciones sin comprometer la seguridad de la información.
- Revisión y mejora continua de los procedimientos para optimizar la eficiencia operativa y minimizar los riesgos asociados a la manipulación de datos.

c. Controles Técnicos y Procedimentales:

- Implementación de controles técnicos, como firewalls, sistemas de detección de intrusiones y cifrado, para salvaguardar la integridad y confidencialidad de la información.
- Desarrollo de procedimientos detallados que establezcan pautas claras y prácticas seguras para el manejo de la información.

d. Concienciación y Capacitación:

- Diseño e implementación de programas de concienciación y capacitación para todo el personal, con el objetivo de promover una comprensión profunda de los riesgos de seguridad de la información y fomentar prácticas seguras.

e. Responsabilidades y Compromisos:

- Definición de roles y responsabilidades claros en relación con la seguridad de la información, desde las máximas autoridades hasta el personal operativo.
- Aseguramiento del compromiso manifiesto de las autoridades y líderes de las unidades para difundir y cumplir con las políticas establecidas.

f. Cultura Organizacional:

- Integración de los principios de seguridad de la información en la cultura organizacional, buscando la internalización de estas prácticas en las acciones cotidianas y en la toma de decisiones.

- Promoción de una cultura de responsabilidad y reporte proactivo de incidentes de seguridad.

Este alcance integral busca garantizar que las políticas de seguridad de la información se conviertan en un componente esencial y transversal de las operaciones del Servicio Nacional Textil, fortaleciendo la resiliencia organizacional y asegurando la protección efectiva de la información crítica.

4.6. ROLES Y RESPONSABILIDADES

En el marco de la Política de Seguridad de la Información del Servicio Nacional Textil, se establecen roles y responsabilidades claramente definidos para garantizar la efectiva implementación y cumplimiento de las medidas de seguridad.

i. Comité de Seguridad de la Información - CSI

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 métricas 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.

ii. Responsable de Seguridad de la Información - RSI

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 Políticas 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 práctica 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) Promover 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.

iii. Responsabilidades de la Máxima Autoridad Ejecutiva

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

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

s) Designar al responsable de Seguridad de la Información (RSI).

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

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

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

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

x) Cumplir y hacer cumplir el Plan Institucional de seguridad de la Información.

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

iv. Todo el Personal del SENATEX

Cada miembro, independientemente de su posición o función, incluyendo autoridades ejecutivas y personal profesional - técnico, tiene la responsabilidad directa de implementar supervise el cumplimiento de la Política de Seguridad de la Información en sus unidades organizacionales, promoviendo una cultura organizacional comprometida con la seguridad de la información.

Esta clara distribución de roles y responsabilidades pretende establecer una estructura organizativa sólida, donde la colaboración activa de todos los niveles garantice la eficacia de la Política de Seguridad de la Información y contribuya a la creación de un entorno seguro y resiliente.

4.7. DESARROLLO

La PSI establece posturas institucionales respecto al Plan Institucional de Seguridad de la Información, tomando los resultados obtenidos y controles mínimos de seguridad contemplados de acuerdo al análisis de riesgo realizado en los distintos ámbitos de seguridad con los siguientes resultados:

1	SEGURIDAD EN RECURSOS HUMANOS
	POSTURA INSTITUCIONAL
	La institución reconoce la imperiosa necesidad de instaurar mecanismos de relación efectivos entre el recurso humano y la entidad en el ámbito de seguridad de la información. Este enfoque busca salvaguardar la integridad y confidencialidad de la información a la cual el personal tiene acceso, tanto durante su vinculación laboral como en el período posterior.
	ACTIVIDADES CLAVE
	1.1. Capacitar y Sensibilizar en seguridad de la información acerca de los riesgos y protocolos de seguridad, fomentando una cultura organizacional arraigada en la responsabilidad individual y colectiva en el manejo de la información.
	1.2. Gestionar de manera responsable los accesos a la información, limitando el alcance a lo estrictamente necesario para el desempeño de las funciones laborales de cada individuo.
	1.3. Establecer procedimientos y/o acuerdos que aseguren el cumplimiento continuo de las políticas de seguridad de la información incluso después de la finalización

de la vinculación laboral, protegiendo así la información sensible de la institución.

2 GESTIÓN DE ACTIVOS DE INFORMACIÓN

POSTURA INSTITUCIONAL

La institución asume un compromiso firme con la preservación de la integridad, disponibilidad y confidencialidad de sus activos de información. Reconociendo la importancia estratégica de estos activos, la postura institucional hacia la política de seguridad de la información que se enfoca en una gestión proactiva, controlada y responsable de dichos activos.

ACTIVIDADES CLAVE

2.1. Establecer controles y/o protocolos específicos para la gestión de activos, abarcando desde la asignación de responsabilidades hasta la implementación de medidas técnicas y procedimentales que aseguren su protección.
2.2. Mantener un inventario actualizado y garantizar la eliminación segura de todos los activos de información, ya sea hardware o documentos confidenciales.
2.3. Implementar mecanismos de monitoreo continuo para evaluar el estado y la seguridad de los activos de información, identificando y respondiendo proactivamente a posibles amenazas o vulnerabilidades.
2.4. Realizar copias de seguridad periódicas de los activos críticos y tener un plan de recuperación ante desastres.

3 CONTROL DE ACCESOS

POSTURA INSTITUCIONAL

La institución adopta una postura proactiva y estratégica en relación con el control de accesos, reconociendo que la gestión efectiva de este aspecto es esencial para preservar la seguridad y confidencialidad de la información, con el objetivo de garantizar un control robusto y adecuado.

ACTIVIDADES CLAVE

3.1. Establecer políticas y/o reglas claras que definan quién tiene acceso a qué recursos, los niveles de acceso y las circunstancias bajo las cuales se otorgan o revocan los permisos.
3.2. Establecer políticas y/o reglas claras que definan quién tiene acceso a qué recursos, los niveles de acceso y las circunstancias bajo las cuales se otorgan o revocan los permisos.

3.3. Adoptar el principio de menor privilegio, limitando los accesos y asignando privilegios mínimos necesarios para que los usuarios desempeñen sus funciones, reduciendo así la superficie de exposición a posibles amenazas.

3.4. Implementar políticas y/o procedimientos para la revocación inmediata de accesos en caso de cambios en el estatus laboral o responsabilidades del usuario, minimizando el riesgo asociado con accesos no autorizados.

4 CRIPTOGRAFÍA

POSTURA INSTITUCIONAL

La institución reconoce la criptografía como un pilar esencial en la salvaguarda de la información, adoptando una postura estratégica que promueve su utilización para fortalecer la confidencialidad, autenticidad, integridad, no repudio y autenticación de la información.

ACTIVIDADES CLAVE

4.1. Gestionar la adquisición de Tecnologías de Información para Cifrado correspondiente, así poder iniciar con las acciones pertinentes a la criptografía en la institución.

5 SEGURIDAD FÍSICA Y AMBIENTAL

POSTURA INSTITUCIONAL

La institución asume un compromiso integral con la seguridad de la información, reconociendo que la protección de áreas e instalaciones físicas es esencial para salvaguardar la integridad, confidencialidad y disponibilidad de la información sensible y crítica.

ACTIVIDADES CLAVE

5.1. Mantener servidores, dispositivos de almacenamiento y otros equipos críticos en áreas seguras y protegidas.

5.2. Implementar fuentes de energía alternativas, así como sistemas de respaldo, para garantizar la continuidad de las operaciones incluso en casos de cortes de energía.

5.3. Implementar protocolos de respuesta ante emergencias y/o procedimientos de evacuación, respecto medidas de seguridad física y ambiental.

6	SEGURIDAD DE LAS OPERACIONES

POSTURA INSTITUCIONAL

La institución adopta una postura proactiva y estratégica en relación con el control de seguridad de las operaciones, reconociendo que la correcta ejecución de las actividades operacionales en instalaciones de procesamiento de información es fundamental para la seguridad de la información, comprometiéndose con la excelencia operacional e integración con la estrategia institucional.

ACTIVIDADES CLAVE

6.1. Implementar procedimiento y/o plan detallado para manejar incidentes de seguridad, incluyendo cómo responder a brechas de seguridad, ataques cibernéticos, o fallos de sistemas.
6.2. Implementar Programas de Mantenimiento Preventivo en el área de tecnologías de información para reducir vulnerabilidades.

7	SEGURIDAD DE LAS COMUNICACIONES

POSTURA INSTITUCIONAL

La institución adopta una postura estratégica y proactiva en relación con el control de seguridad de las comunicaciones, reconociendo que la protección de la información transmitida a través de las redes de datos es esencial para salvaguardar su integridad, confidencialidad y disponibilidad.

ACTIVIDADES CLAVE

7.1. Implementar protocolos de seguridad específicos para las comunicaciones, abordando aspectos como la autenticación, el cifrado, la integridad de los datos transmitidos, ataques cibernéticos, como firewalls y sistemas de detección de intrusiones, para mitigar riesgos y garantizar la integridad de las comunicaciones.
7.2. Formalizar e implementar seguridad para el Correo Electrónico.

8	DESARROLLO, MANTENIMIENTO Y ADQUISICIÓN DE SISTEMAS

POSTURA INSTITUCIONAL

La institución adopta una postura estratégica y proactiva en relación con el control de desarrollo, mantenimiento y adquisición de sistemas, reconociendo que este

	proceso es crítico para garantizar la seguridad de la información en todas las fases del ciclo de vida del sistema.
	ACTIVIDADES CLAVE
	8.1. Reforzar al área de sistemas con personal idóneo para el desarrollo de sistemas de información y tomar acción oportuna en lo que se requiera. **8.2.** Elaborar un reglamento y/o procedimiento el mantenimiento de sistemas. **8.3.** Establecer procesos y/o procedimientos para la realización de copias de seguridad.
9	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
	POSTURA INSTITUCIONAL
	La institución adopta una postura proactiva y estratégica en relación con la gestión de incidentes de seguridad de la información, reconociendo la importancia crítica de responder rápidamente a eventos adversos para garantizar la continuidad operativa y fortalecer los controles de seguridad implementados.
	ACTIVIDADES CLAVE
	9.1. Implementar un Plan de Respuesta a Incidentes.
10	**PLAN DE CONTINGENCIAS TECNOLÓGICAS**
	POSTURA INSTITUCIONAL
	La institución adopta una postura estratégica y proactiva en relación con el control del Plan de Contingencias Tecnológicas, reconociendo la importancia crítica de tener medidas estructuradas y efectivas para responder a incidentes de seguridad de la información y situaciones de emergencia.
	ACTIVIDADES CLAVE
	10.1. Implementar un Plan de Contingencias Tecnológicas.
11	**CUMPLIMIENTO**
	POSTURA INSTITUCIONAL
	La institución adopta una postura firme y proactiva para garantizar el cumplimiento operativo del Plan Institucional de Seguridad de la Información, el cual engloba la

Política de Seguridad de la Información y la documentación resultante de la misma. Esta postura refleja el compromiso de la organización con la protección efectiva de la información y la gestión integral de riesgos asociados.
ACTIVIDADES CLAVE
11.1. Capacitación y difusión del Plan Institucional de Seguridad de la Información, el cual engloba la Política de Seguridad de la Información.
11.2. Establecer indicadores y métricas de cumplimiento al momento de elaborar y desarrollar un determinado control de seguridad.
11.3. Realizar revisiones periódicas a los controles implementados de acuerdo al cumplimiento operativo del Plan Institucional del Seguridad de la Información que conlleva la Política de Seguridad de la Información y la documentación resultante de la misma.

4.8. DIFUSIÓN

La Política de Seguridad de Información, se difundirá, se hará seguimiento y cumplimiento de manera específica a todas las áreas y a los servidores específicos encargados de su implementación.

4.9. CUMPLIMIENTO

La presente Política de Seguridad de Información es de cumplimiento obligatorio para todo el personal dependiente del Servicio Nacional Textil - SENATEX.

4.10. SANCIONES

El incumplimiento o la violación de las disposiciones de la presente Política de Seguridad de Información y los potenciales efectos adversos para la organización serán valorados en aplicación del Reglamento Interno de Personal del Servicio Nacional Textil - SENATEX, específicamente en cuanto a:

- Artículo 11 (DEBERES CON LA ENTIDAD), que en el inciso c) señala:

  "Desarrollar sus labores o tareas y manejar la documentación e información a su cargo con responsabilidad y diligencia".

- Artículo 41 (FALTAS Y SANCIONES) que indica:

  I. Las faltas cometidas por el personal de la entidad en contra de lo establecido por el presente Reglamento Interno, así como a la normativa jurídica y administrativa para el sector público, se calificarán en función al grado de afectación que estas tengan sobre la gestión pública de la entidad, así como por su recurrencia.

4.11. HISTÓRICO DE CAMBIOS

Se recomienda que la documentación generada a partir de la PSI cuente con el respectivo control de cambios, el cual consigne información referente a:

- Versión del documento
- Modificación del documento
- Personal encargado de la modificación.
- Identificar una nueva versión del documento.
- Documentar el control de cambios de acuerdo a las versiones de la planificación.

4.12. CRONOGRAMA DE IMPLEMENTACIÓN

INICIO	FIN	CONTROLES A IMPLEMENTARSE	ROLES Y RESPONSABILIDADES (4,6, DESARROLLO)	APOYO PARA IMPLEMENTACIÓN	ACTIVIDADES (4,7, DESARROLLO)	2023 NOV	2023 DIC	2024 ENE	2024 FEB	2024 MAR	2024 ABR	2024 MAY	2024 JUN	2024 JUL	2024 AGO	2024 SEP	2024 OCT
1-11-23	29-2-24	SEGURIDAD EN RECURSOS HUMANOS	**RSI:** Numeral ii. incisos d), e), f), g), j), l), o) y p) **CSI:** Numeral i. incisos c), d), e) y f)	**SISTEMAS:** Coadyuvar en la implementación técnica. **RECURSOS HUMANOS:** Coadyuvar en la implementación operativa.	**1.1., 1.2. y 1.3.**												
2-1-24	1-5-24	GESTIÓN DE ACTIVOS DE INFORMACIÓN	**RSI:** Numeral ii. incisos d), e), f), g), j), l), o) y p) **CSI:** Numeral i. incisos c), d), e) y f)	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**2.1., 2.2., 2.3. y 2.4.**												
1-3-24	29-6-24	CONTROL DE ACCESOS	**RSI:** Numeral ii. incisos d), e), f), g), j), l), o) y p) **CSI:** Numeral i. incisos c), d), e) y f)	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**3.1., 3.2. y 3.3.**												
1-6-24	31-7-24	CRIPTOGRAFÍA	**RSI:** Numeral ii. incisos d), e), f), g), j), l), o) y p) **CSI:** Numeral i. incisos c), d), e) y f)	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**4.1.**												

INICIO	FIN	CONTROLES A IMPLEMENTARSE	ROLES Y RESPONSABILIDADES (4,6, DESARROLLO)	APOYO PARA IMPLEMENTACIÓN	ACTIVIDADES (4,7, DESARROLLO)	2023 NOV	2023 DIC	2024 ENE	2024 FEB	2024 MAR	2024 ABR	2024 MAY	2024 JUN	2024 JUL	2024 AGO	2024 SEP	2024 OCT
1-5-24	29-8-24	SEGURIDAD FÍSICA Y AMBIENTAL	**RSI:** Numeral ii. incisos d), e), f), g), j), l), o) y p) **CSI:** Numeral i. incisos c), d), e) y f)	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**5.1., 5.2. y 5.3.**												
2-1-24	2-3-24	SEGURIDAD DE LAS OPERACIONES	**RSI:** Numeral ii. incisos d), e), f), g), j), l), o) y p) **CSI:** Numeral i. incisos c), d), e) y f)	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**6.1. y 6.2.**												
1-3-24	30-4-24	SEGURIDAD DE LAS COMUNICACIONES	**RSI:** Numeral ii. incisos d), e), f), g), j), l), o) y p) **CSI:** Numeral i. incisos c), d), e) y f)	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**7.1. y 7.2.**												
1-5-24	30-6-24	DESARROLLO, MANTENIMIENTO Y ADQUISICIÓN DE SISTEMAS	**RSI:** Numeral ii. incisos d), e), f), g), j), l), o) y p) **CSI:** Numeral i. incisos c), d), e) y f)	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**8.1., 8.2. y 8.3.**												
1-9-24	1-10-24	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	**RSI:** Numeral ii. incisos d), e), f), g), h), i), j), l), o) y p) **CSI:** Numeral i.	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**9.1.**												

						2023		2024									
INICIO	FIN	CONTROLES A IMPLEMENTARSE	ROLES Y RESPONSABILIDADES (4,6, DESARROLLO)	APOYO PARA IMPLEMENTACIÓN	ACTIVIDADES (4,7, DESARROLLO)	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT
			incisos c), d), e), f) y g)														
1-10-24	31-10-24	PLAN DE CONTINGENCIAS TECNOLÓGICAS	**RSI:** Numeral ii. incisos d), e), f), g), i), j), l), o) y p) **CSI:** Numeral i. incisos c), d), e) y f)	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**10.1.**												
1-11-23	31-10-24	CUMPLIMIENTO	**RSI:** Numeral ii. incisos d), e), f), g), h), i), j), l), m), n), o) y p)**CSI:** Numeral i. incisos c), d), e), f), g) y h)	**SISTEMAS:** Coadyuvar en la implementación técnica y operativa.	**11.1., 11.2. y 11.3.**												