RESOLUCIÓN ADMINISTRATIVA MFSJ N° 033/2023

La Paz, 05 de septiembre de 2023

VISTOS:

La Hoja de Ruta SEPDEP-UI-9324-2023, Informe SEPDEP-UI-INF-Z-45-2023 de fecha 31 de agosto de 2023, Informe Legal SPDP/AL/LJTM/Nº 162/2023 de 05 de septiembre de 2023 y todos los demás antecedentes:

CONSIDERANDO:

Que, el Servicio Plurinacional de Defensa Pública, bajo tuición del Ministerio de Justicia y Transparencia Institucional, como institución descentralizada encargada del régimen de defensa penal pública de las personas denunciadas, imputadas o procesadas penalmente, conforme lo establecido por la Ley Nº 463, busca contribuir a la implementación de las reformas orientadas a mejorar el acceso a la justicia, haciendo énfasis en los grupos más vulnerables de la sociedad con un enfoque de derechos humanos y género, procurando brindar la oportunidad real de toda persona imputada a contar con los medios adecuados y el tiempo necesario para ejercer su defensa en todo proceso, misma que constituye una garantía inviolable que permiten concretar el debido proceso e imparcialidad, las condiciones de igualdad jurídica, un proceso pronto y oportuno, acceder a la defensa técnica y el respeto y vigencia de los derechos y garantías sustanciales procesales.

Que, el aartículo 29 de la Ley Nº 463 establece como atribuciones de la Directora Nacional "1. Dirigir, organizar y administrar el Servicio. 2. Representar judicial y ejecutivamente a la institución. (...) 5. Fijar los criterios que se aplicarán en materia de recursos humanos, remuneraciones, inversiones, gastos, planificación, administración y finanzas. (...) 28. Otras atribuciones establecidas por Ley.".

Que, la Ley Nº 463 del Servicio Plurinacional de Defensa Pública de 19 de diciembre de 2013, establece en su Artículo 26 que la Directora Nacional es la Máxima Autoridad del Servicio Plurinacional de Defensa Pública.

Que, mediante Resolución Ministerial Nº 108/2020 de 13 de noviembre de 2020, del Ministerio de Justicia y Transparencia Institucional, se Designa como directora Nacional del Servicio Plurinacional de Defensa Pública a la ciudadana Marcela Filma Siles Jaksic con C.I. Nro. 3098580 Oruro.

CONSIDERANDO:

Que, la Ley N° 650 de 15 de enero de 2015, en su artículo 1 eleva a rango de Ley la "Agenda Patriótica del Bicentenario 2025", que contiene trece pilares de la Bolivia Digna y Soberana; cuyo Pilar 4: Soberanía científica y tecnológica con identidad propia; establece 5 metas.

Que, la Ley Nº 164 General de Telecomunicaciones, Tecnologías de Información y Comunicación, en su Artículo 2 numeral 5 plantea como uno de sus objetivos el "Promover el uso de las tecnologías de información y comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos.".

Que, en el ámbito del fortalecimiento tecnológico, la referida norma en su artículo 7 numeral 1 parágrafo I plantea: "Formular políticas, planes y programas que garanticen a través del uso de las telecomunicaciones y tecnologías de información y comunicación, el mejoramiento de la calidad de vida de las bolivianas y los bolivianos y el acceso equitativo a oportunidades de educación, salud y cultura, entre otras."

Que, el artículo 72 parágrafos I y II disponen 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." y "Las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las tecnologías de información y comunicación en el desarrollo de sus funciones."

Que, el Decreto Supremo N° 2514 en su Artículo 8 parágrafo I crea el Centro de Gestión de Incidentes Informáticos (CGII) como parte de la estructura técnico operativa de la AGETIC; en su parágrafo II establece entre sus funciones "c. Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público;" y "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;"

Que, el artículo 9 de la referida norma crea el Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB), como instancia de coordinación para la implementación de Gobierno Electrónico y para el uso y desarrollo de Tecnologías de Información y Comunicación.

Que, el artículo 17 en su parágrafo III establece como obligaciones en materia de Seguridad Informática que "Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII.".

Que, mediante Resolución Administrativa AGETIC/RA/0051/2017 de 19 de Septiembre de 2017, se aprueba los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público" y sus tres Anexos.

Que, el referido documento señala en su numeral 6 "Lineamientos para la elaboración del PISI", que el proceso de elaboración del Planes Institucionales de Seguridad de la Información (PISI) se desarrolla por etapas, siendo la Etapa Inicial responsabilidad de la Máxima Autoridad Ejecutiva de la entidad, misma que consta de dos actividades: 1. Designación del Responsable de Seguridad de la Información y 2. Conformación del Comité de Seguridad de la Información.

Que, en su numeral 6.1.3 Conformación y funciones del Comité de Seguridad de Información (CSI) establecen que "Mediante Resolución Administrativa, la Máxima Autoridad Ejecutiva designará al personal que conformará el Comité de Seguridad de la Información (CSI), de acuerdo al tamaño de la estructura organizativa de su entidad, volumen y complejidad de sus operaciones." Asimismo, se menciona que el Comité de Seguridad de la Información establecerá su organización interna y asumirá como mínimo las siguientes funciones: a) Revisar el Plan Institucional de Seguridad de la Información (PSI); b) Promoverá la aprobación del PISI a través de la MAE (...)". De la misma forma, en su numeral 6.4. Aprobación del PSI 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".

CONSIDERANDO:

Que, mediante Resolución Administrativa MFSJ N° 030/2023 de 30 agosto de 2023, se Resuelve: "PRIMERO.- DESIGNAR Y RATIFICAR a los siguientes miembros del Comité de Seguridad de la Información: Lic. Juan Pablo Rojas Colquechambi - Director Administrativo Financiero; Lic. Lic. Gonzalo Mauricio Martin Linares Valdez - Responsable de Planificación y Difusión; Ing. Octavio Jesús Torrico Álvarez - Encargado de Informática; Elena Fabiola Fernández Pacamía – Defensora Público. SEGUNDO.- CONFORMAR el Comité de Seguridad de la Información de la siguiente manera: Presidente: Lic. Juan Pablo Rojas Colquechambi; Responsable de Seguridad de la Información (RSI): Ing. Octavio Jesús Torrico Álvarez; Secretario: Lic. Gonzalo Mauricio Martin Linares Valdez y Miembro: Abog. Elena Fabiola Fernández Pacamía".

Que, mediante Informe SEPDEP-UI-INF-Z-45-2023 de fecha 31 de agosto de 2023, remitido por el Comité de la Seguridad de la Información del SEPDEP, con referencia "Aprobación del Plan Institucional de la Seguridad de la Información", señalan que el Comité de la Seguridad de la Información realizó una reunión de fecha 31 de agosto del 2023 para revisar y aprobar el Plan Institucional del Servicio Plurinacional de Defensa Pública.

Que, mediante Informe Legal SPDP/AL/LJTM/N° 162/2023 de fecha 05 de septiembre de 2023, emitido por el Abog. Luis Juan Tola Mamani – Asesor Legal del SEPDEP, se concluye que: "1. De acuerdo a la Resolución Administrativa MFSJ N° 030/2023 de agosto de 2023, emitido por su autoridad como Directora Nacional del Servicio Plurinacional de Defensa Pública Resuelve: "PRIMERO.- DESIGNAR Y RATIFICAR a los siguientes miembros del Comité de Seguridad de la Información: Lic. Juan Pablo Rojas Colquechambi - Director Administrativo Financiero; Lic. Lic. Gonzalo Mauricio Martin Linares Valdez - Responsable de Planificación y Difusión; Ing. Octavio Jesús Torrico Álvarez - Encargado de Informática; Elena Fabiola Fernández Pacamía – Defensora Público. SEGUNDO.- CONFORMAR el Comité de Seguridad de la Información de la siguiente manera: Presidente: Lic. Juan Pablo Rojas Colquechambi; Responsable de Seguridad de la Información (RSI): Ing. Octavio Jesús Torrico Álvarez; Secretario: Lic. Gonzalo Mauricio Martin Linares Valdez y Miembro: Abog. Elena Fabiola Fernández Pacamía. 2. Mediante Informe SEPDEP-UI-INF-Z-45-2023 de fecha 31 de agosto de 2023, remitido por el Comité de la Seguridad de la Información del SEPDEP, a su autoridad con referencia "Aprobación del Plan Institucional de la Seguridad de la Información", concluye que: "el Plan Institucional de la seguridad de la Información gestión 2023-2024 se encuentra terminado y aprobado por el Comité de la Seguridad de la Información". Recomendando: "en cumplimiento a los lineamientos del Plan Institucional de la Seguridad de la Información, se apruebe el Plan Institucional de la Seguridad de la Información mediante Resolución Administrativa, posteriormente emitir una copia a la Agencia de gobierno electrónico y tecnologías de información y comunicación AGETIC".

Recomendando: "1. Aprobar el Informe SEPDEP-UI-INF-Z-45-2023 de fecha 31 de agosto de 2023, remitido por el Comité de la Seguridad de la Información del SEPDEP, con referencia "Aprobación del Plan Institucional de la Seguridad de la Información. 2. Suscribir Resolución Administrativa para la aprobación del Plan Institucional de Seguridad de la Información del Servicio Plurinacional de Defensa Pública público Versión 1.3, y Anexo conforme establece los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector en su punto 6.1.3 y 6.4. misma que no vulnera normativa legal vigente. 3. Notificar con una copia de la Resolución Administrativa a los miembros del Comité de la Seguridad de la Información del SEPDEP. Remitir una copia de la presente Resolución Administrativa a la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación".

POR TANTO:

La Directora Nacional del Servicio Plurinacional de Defensa Pública, en uso de las atribuciones conferidas en los numerales 1, 2 y 28 del artículo 29 de la Ley N° 463 del 19 de diciembre de 2013.

RESUELVE:

PRIMERO. - Aprobar el **Informe SEPDEP-UI-INF-Z-45-2023** de fecha 31 de agosto de 2023, emitido por el Comité de la Seguridad de la Información del SEPDEP, con referencia **"Aprobación del Plan Institucional de la Seguridad de la Información** y el **Informe Legal SPDP/AL/LJTM/N° 162/2023** de fecha 05 de septiembre de 2023, emitido por Asesoría Legal del SEPDEP.

SEGUNDO. – Aprobar el **Plan Institucional de Seguridad de la Información del Servicio Plurinacional de Defensa Pública público Versión 1.3, y Anexo,** conforme establece el **Informe SEPDEP-UI-INF-Z-45-2023** de fecha 31 de agosto de 2023, emitido por el Comité de la Seguridad de la Información del SEPDEP y los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector en sus puntos 6.1.3 y 6.4.

TERCERO.- Encargar al **Comité de la Seguridad de la Información del SEPDEP**, la aplicación, ejecución y cumplimiento del **Plan Institucional de la Seguridad de la Información del Servicio Plurinacional de Defensa Pública,** bajo estricta observancia de las normas vigentes.

CUARTO.- Notificar con una copia de la Resolución Administrativa a los miembros del **Comité de la Seguridad de la Información del SEPDEP**.

QUINTO.- Remitir una copia de la presente Resolución Administrativa a la **Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación.**

Regístrese, comuníquese, cúmplase y archívese.

Abog. Marcela Filma Siles Jaksic
DIRECTORA NACIONAL
Servicio Plurinacional de Defensa Pública
MINISTERIO DE JUSTICIA Y TRANSPARENCIA INSTITUCIONAL

Abog. [illegible] Toro Mamani
ASESOR LEGAL
SERVICIO PLURINACIONAL DE DEFENSA PÚBLICA
MINISTERIO DE JUSTICIA Y TRANSPARENCIA INSTITUCIONAL

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DEL

SERVICIO PLURINACIONAL DE DEFENSA PÚBLICA

Versión: 1.3

Nombre de la Entidad: Servicio Plurinacional de Defensa Pública

Dirección: Calle Batallón Colorados, Edif. “El Cóndor” Piso 13

Dirección Web: www.sepdep.gob.bo

Fecha de Finalización: 31/08/2023

Elaborado por el RSI: Ing. Octavio Jesús Torrico Alvarez

Revisado y aprobado por el Comité de la Seguridad de la Información

Servicio Plurinacional de Defensa Pública

Políticas de Seguridad

Introducción

La información es un activo que tiene un valor incalculable para las instituciones, tanto privadas como públicas, en la actualidad nos encontramos amenazados por riesgos que ponen en peligro esta información.
Bajo tal premisa, la seguridad de la información es la protección de la información contra una amplia gama de amenazas con el fin de garantizar la continuidad de la entidad, minimizar los riesgos institucionales y maximizar resultados y oportunidades.
El Estado Plurinacional de Bolivia administra información de la ciudadanía en general, por tanto, debe ser responsable por su seguridad. Es así que la Ley N° 650 de 15 de enero de 2015, que en su artículo 1 eleva a rango de Ley la "Agenda Patriótica del Bicentenario 2025", contiene trece pilares de la Bolivia Digna y Soberana; cuyo Pilar 4: Soberanía científica y tecnológica con identidad propia; establece 5 metas.

Asimismo, la Ley Nº164 General de Telecomunicaciones, Tecnologías de Información y Comunicación, en su Artículo 2 numeral 5 plantea como uno de sus objetivos el "Promover el uso de las tecnologías de información y comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos.". En el ámbito del fortalecimiento tecnológico, la referida norma, en su Artículo 7, numeral 1 parágrafo I plantea: "Formular políticas, planes y programas que garanticen a través del uso de las telecomunicaciones y tecnologías de información y comunicación, el mejoramiento de la calidad de vida de las bolivianas y los bolivianos y el acceso equitativo a oportunidades de educación, salud y cultura, entre otras."
Consecuentemente, su artículo 72 parágrafos I y II disponen 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." y "Las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las tecnologías de información y comunicación en el desarrollo de sus funciones."

Mediante Decreto Supremo N°1793 de 13 de noviembre de 2013 se aprueba el Reglamento a la Ley Nº 164, de 8 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación, cuyo inciso d) del Artículo 4 (Principios), parágrafo II, señala que: "Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento". Por su parte, el Artículo 8 (Plan de contingencia) dispone que: "Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad".

Por otra parte, el Artículo 8 del Decreto Supremo N°2514 de 9 de septiembre de 2015 en su parágrafo I crea el Centro de Gestión de Incidentes Informáticos (CGII) como parte de la estructura técnico operativa de la AGETIC; en su parágrafo II establece entre sus funciones: "c. Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público;". Asimismo, el Artículo 9 de la referida norma crea el Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB), como instancia de coordinación para la implementación de Gobierno Electrónico y para el uso y desarrollo de Tecnologías de Información y Comunicación. En concordancia con lo señalado, el Artículo 17 en su parágrafo III establece como obligaciones en materia de Seguridad Informática que "Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII.".

Bajo tales previsiones, el Servicio Plurinacional de Defensa Pública, en cumplimiento de la normativa para la Implementación de Políticas de Seguridad de la Información, debe garantizar la infraestructura, equipamiento y financiamiento necesario para su ejecución. Para este efecto, los aspectos administrativos, tecnológicos y operativos serán controlados y protegidos, promoviendo la preparación del Plan de Implementación de Seguridad de la Información (PISI) de cumplimiento obligatorio.

Términos y Definiciones

SEPDEP: Garantizar la inviolabilidad del derecho a la defensa y el acceso a una justicia oportuna y gratuita, prestando servicios de asistencia técnica y defensa penal a toda persona denunciada, imputada o procesada penalmente, carente de recursos económicos y a quienes no designen abogado para su defensa.

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.

Confidencialidad: Propiedad por la cual la información no esté disponible o divulgada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad por la cual se tiene acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requiera.

Integridad: La propiedad de salvaguardar la exactitud, completitud de la información y los métodos de procesamiento.

No repudio: La garantía de que el remitente de la información ha proporcionado el comprobante de entrega y el destinatario ha proporcionado la prueba de la identidad del remitente, de tal manera que ninguno pueda negar el origen 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.

Trazabilidad: Capacidad de registro del manejo de la información, de manera que cualquier operación pueda ser rastreada hasta su origen. Esto apoya el no repudio, la disuasión, el aislamiento de fallos, la detección y prevención de intrusiones para luego realizar gestiones de recuperación y acciones legales.

Contraseñas Robustas: Una contraseña robusta es la que está diseñada para que sea difícil de descubrir para una persona o un programa. Ya que el propósito de una contraseña es asegurar que solo los usuarios autorizados pueden acceder a los recursos, una contraseña que es fácil de adivinar es un riesgo de seguridad.
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
CCTV.- (en inglés closed circuit television) es una tecnología de videovigilancia diseñada para supervisar una diversidad de ambientes y actividades.

VPN.- Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN) es una tecnolo-gía 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.

IPS.- El proveedor de servicios de Internet, (ISP, por la sigla en inglés de Internet service provi-der) es la empresa que brinda conexión a Internet a sus clientes.

Objetivo general

Implementar una guía de procedimientos para la implantación de medidas de seguridad de la información generada por los distintos activos de información identificados en el Servicio Plurinacional de Defensa Pública, en estricto apego a el Decreto Supremo N°2514 de 9 de septiembre de 2015 disposición transitoria segunda.

Objetivos específicos

- Promover y generar una mayor conciencia sobre la importancia de la seguridad de la información involucrando a las distintas áreas de la entidad en la elaboración e implantación de las distintas medidas de seguridad.
- Generar los controles mínimos para la seguridad de la información.
- Generar una política de seguridad de la información que sirva como línea base institucional para la generación de normativa interna.
- Establecer un cronograma de control de la información.
- Realizar relevamiento de la información en las diferentes áreas.
- Comprender y tratar los riesgos operacionales y estratégicos en seguridad de la información para que permanezcan en niveles aceptables para la entidad.
- La protección de la confidencialidad de la información relacionada con los usuarios del Servicio.
- La conservación de la integridad de los registros contables.
- Los servicios Web de acceso público y las redes internas cumplan con las especificaciones de seguridad requeridas.

Alcance

La Política de Seguridad de la Información (PISI) tiene como alcance y ámbito de aplicación a toda la Dirección del Servicio Plurinacional de Defensa Pública, incluyendo todos los recursos de información sean estos tangibles como los recursos tecnológicos y de comunicación, e intangibles como información del servidor público, relación con proveedores, personal temporal, institucional y otros.

Roles y Responsabilidades

el cumplimiento de la PISI.

Directores, Jefes y Responsables de Unidad

- Son propietarios de los activos de información y procesos bajo su dependencia.

• Son responsables de realizar la evaluación de riesgos de los activos de su propie-dad, en coordinación con el Responsable de Seguridad de la Información (RSI).

• Son responsables de identificar las necesidades o cambios a los documentos normativos internos que incorporen aspectos de seguridad de la información ajus-tados a sus activos de información o procesos relacionados a los mismos.

• Son responsables de verificar el cumplimiento de la PISI en sus Unidades Orga-nizacionales.

Personal de SEPDEP

Son responsables del conocimiento y cumplimiento de la presente política en el marco de los procesos de seguridad de la información establecidos en la PISI del SEPEP.

Comité de Seguridad de la Información

Es responsable de analizar, evaluar y revisar las estrategias de seguridad de la informa-ción de la DIRNOPLU a propuesta del RSI para ser puesta a consideración de la Direc-ción Ejecutiva para su aprobación.

Responsable Seguridad de la Información

a) Elaborar estrategias de seguridad de la información del SEPDEP, gestionar su implementación, realizar seguimiento y avaluación de resultados.

b) Revisar la PISI periódicamente y actualizarla ante cambios significativos o necesi-dades institucionales.

c) Capacitar y concientizar sobre aspectos de seguridad de la información y para el cumplimiento de la PISI a todo el personal del SEPDEP.

d) Realizar el seguimiento y monitoreo del cumplimiento de la PISI.

Desarrollo

Ámbito de Seguridad / Descripción	Postura Institucional	Estado
1. Seguridad en recursos humanos Es necesario establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y la entidad o institución pública con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral.	Descripción: Se implementarán controles para la protección de la información institucional ante amenazas que se originan del recurso humano. Postura: El SEPDEP a través de las instancias correspondientes informará, concretizará y evaluará los conocimientos necesarios sobre la seguridad de la información al personal de la institución.	No Utiliza
2. Gestión de activos de información Con el fin de preservar la integridad, disponibilidad y confidencialidad de los activos de información, se debe administrar, controlar y asignar responsabilidades en el uso y protección de los mismos.	Descripción: Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta. Postura: El SEPDEP, identificará los recursos críticos, procesos y procedimientos operacionales para ser formalizados a través de documentos fácilmente entendibles, garantizando de esta manera la continuidad del desarrollo de estos recursos identificados.	Utiliza
3. Control de accesos Gestionar los accesos a servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario.	Descripción: Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones de la institución reflejada en documentos de respaldo. Postura: El SEPDEP, elaborará procesos, procedimientos y reglamentos relacionados a las redes de telecomunicación y dispositivos utilizados por la institución, para precautelar y garantizar la continuidad de las comunicaciones.	Utiliza
4. Criptografía El uso de técnicas criptográficas aporta mayores niveles de seguridad para proteger la confidencialidad, autenticidad e integridad de la información, además del no repudio y	Descripción: Se refiere al uso de técnicas criptográficas para aportar mayores niveles de seguridad en la protección de la confidencialidad, autenticidad e integridad de la información, además del no repudio y autenticación.	No Utiliza

Ámbito de Seguridad / Descripción	Postura Institucional	Estado
autenticación.	Postura: El SEPDEP, impulsara el uso de medios criptográficos, así como la firma digital en sus procesos y procedimientos internos e interinstitucionales.	
5. Seguridad física y ambiental Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica para la entidad o institución pública, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.	Descripción: Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y crítica para la SEPDEP, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información. Postura: El SEPDEP, elaborará reglamentos, procesos, procedimientos que permitirán organizar la seguridad física y ambiental donde se encuentren los activos de información, así como su transporte y correcto uso de los mismo. La particularidad del tratamiento de los activos de información en relación a su seguridad física y ambiental, se desprenderá para cada uno de ellos dependiendo el tipo de activo identificado como de su análisis de riesgo correspondiente realizado en la matriz de evaluación de riesgo.	Utiliza
6. Seguridad de las operaciones Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta.	Descripción: Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta. Postura: El SEPDEP, identificará los recursos críticos, procesos y procedimientos operacionales para ser formalizados a través de documentos fácilmente entendibles, garantizando de esta manera la continuidad del desarrollo de estos recursos identificados.	No Utiliza
7. Seguridad de las comunicaciones Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos.	Descripción: Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones de la institución reflejada en documentos de respaldo. Postura: El SEPDEP, elaborará procesos, procedimientos y reglamentos relacionados a las redes de telecomunicación y dispositivos utilizados por la institución, para precautelar y garantizar la continuidad de las comunicaciones.	Utiliza
8. Desarrollo, mantenimiento y adquisición de sistemas Establecer requisitos de seguridad para el desarrollo, mantenimiento y adquisición de sistemas que consideren pruebas de seguridad, pruebas de calidad y aceptación para desarrollos internos y externos.	Descripción: Establecer requisitos de seguridad para el desarrollo, mantenimiento y adquisición de sistemas que consideren pruebas de seguridad, pruebas de calidad y aceptación para desarrollos internos y externos de manera segura. Postura: La SEPDEP, elaborará procesos, procedimientos y reglamentos para el desarrollo seguro de aplicación, así como el control de versiones y puestas en producción de los distintos sistemas y aplicaciones tomando en cuenta los códigos fuente, librerías, bases de datos y actualizaciones de software de terceros.	Utiliza
9. Gestión de incidentes de seguridad de la información Establecer mecanismos para la gestión de incidentes en seguridad de la información dentro de la institución o entidad pública para dar continuidad a las operaciones y mejorar los controles de seguridad implementados.	Descripción: Establecer mecanismos para la gestión de incidentes en seguridad de la información dentro de la SEPDEP, para dar continuidad a las operaciones y mejorar los controles de seguridad implementados. Postura: El SEPDEP, implementara mecanismos para garantizar la correcta y oportuna gestión de incidentes que puedan afectar al trabajo y servicios cotidianos de la institución, asignando procedimientos y responsable para la atención de estos incidentes. Asimismo, se realizará la identificación y documentación de los incidentes para mejorar la respuesta a futuras contingencias relacionadas.	No Utiliza

Ámbito de Seguridad / Descripción	Postura Institucional	Estado
10. Plan de contingencias tecnológicas Implementar un Plan de Contingencias Tecnológicas que permita controlar un incidente de seguridad de la información o una situación de emergencia, minimizando sus consecuencias negativas. Asimismo deberá determinar sus requisitos para la seguridad de la información ante situaciones adversas.	Descripción: Implementar un Plan de Contingencias Tecnológicas que permita controlar un incidente de seguridad de la información o una situación de emergencia, minimizando sus consecuencias negativas. Asimismo, deberá determinar sus requisitos para la seguridad de la información ante situaciones adversas. Postura: El SEPDEP, a través de la instancia correspondiente implementara un plan de contingencias tecnológicas, el mismo que se evaluara de forma periódica realizando las pruebas necesarias con el objeto de velicar, revisar y evaluar el mencionado plan.	No Utiliza
11. Cumplimiento Asegurar el cumplimiento operativo del Plan Institucional de Seguridad de la Información que conlleva la Política de Seguridad y la documentación resultante de la misma.	Descripción: Asegurar el cumplimiento operativo del Plan Institucional de Seguridad de la Información que conlleva la Política de Seguridad y la documentación Postura: La SEPDEP, a través de la instancia correspondiente realizará auditorias de cumplimiento a la Política de Seguridad de la Información.	No Utiliza

Difusión

El Plan Institucional de la seguridad de la Información del Servicio Plurinacional de Defensa Pública será difundido en todas la áreas de la intitucuion para su respectiva implementación.

Cumplimiento

El Servicio Plurinacional De Defensa Publica realizara Instructivos a los encargados de cada Área para el cumplimiento del PSI y sobre el formato que tendrá el informe de cumplimiento del mismo.

Sanciones

Ley Nº 1178, Ley Nº 463, Ley de Administración y Control Gubernamental, Reglamento Interno de Personal del SEPDEP

Histórico de Cambios

Fecha	Formulario	Estado	Encargado
2023-08-31	Políticas de Seguridad	EN_REVISION	Octavio Jesús Torrico Álvarez
2023-08-31	Políticas de Seguridad	APROBADO	Comite seguridad de la informacion

Metodología de Gestión de Riesgo

El PISI contempla la gestión de riesgos en el ámbito de la seguridad de la información. Para esto, se adopta la metodología de gestión de riesgos propuesta dentro de los Lineamentos para la Elaboración e Implementeación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, con el objetivo de implementar controles de seguridad o mejorar la eficacia de los controles ya existentes.

La evaluación del riesgo permitirá identificar las debilidades en cuanto a controles de seguridad inexistentes o ineficaces, además de 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.

Identificación, Clasificación y Valoración de Activos de Información

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

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

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

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

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

#	Activo	Descripción	Tipo	Ubicación	Unidad Responzable	Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad	Valoración Final	Fecha inicial	Fecha final
1	Equipos de computación	Equipos de computación asignados al personal de la Institución para el desempeño de sus labores cotidianas.	Equipamiento Informático, Información	Oficina Nacional y Direcciones Departamentales	Activos Fijos y Almacenes	Personal de la Institución al cual se le asignó un equipo de computación	Personal de la Institución al cual se le asignó un equipo de computación.	ALTO	ALTO	ALTO	4.00	2023-09-01	2024-08-31
2	Sistema Informático SISEC v3	Sistema Informático por el cual se tiene un seguimineto de los casos que patricina el Servicio Plurinacional de Defensa Pública	Software - Aplicaciones Informáticas	CPD - Unidad de Informática SEPDEP	Infromatica	Encargado de Informatica	Encargado de Informatica	ALTO	MUY ALTO	ALTO	4.33	2023-09-01	2024-08-31
3	Storage	Discos duros del CPD donde se almacena la informacion de todos los sistemas del SEPDEP	Equipamiento Informático	CPD - Unidad de Informática	Unidad de Informática	Encargado de Informática	Unidad de Informática	MUY ALTO	MUY ALTO	MUY ALTO	5.00	2023-09-01	2024-08-31
4	Equipos Biometricos	Sistema de registro	Equipamiento Informático	Oficina Nacional y Direcciones	Talento Humano	Encargado de Talento Humano	Talento Humano	ALTO	ALTO	BAJO	3.33	2023-09-01	2024-09-01

#	Activo	Descripción	Tipo	Ubicación	Unidad Responzable	Responsable	Custodio	Disponibilidad	Integridad	Confidencialidad	Valoración Final	Fecha inicial	Fecha final
		para el control de asistencia a través de biometría, comprendido por equipos informáticos.		Departamentales									
5	Correo Institucional	Sistema propio de Correo Electrónico Institucional.	Software - Aplicaciones Informáticas	CPD - Unidad de Informatica	Unidad de Informatica	Encargado de Infomatica	Unidad de Informatica	MEDIO	ALTO	ALTO	3.67	2023-09-01	2024-09-01
6	UPS	Equipos con la finalidad de suministrar energía eléctrica en el caso de interrupción eléctrica de la fuente principal.	Equipamiento Informático	CPD - Unidad de Informática	Unidad de infromatica	Encargado de Informatica	Unidad de Informática	MUY ALTO	MEDIO	BAJO	3.33	2023-09-01	2024-09-01
7	Archivo del SEPDEP	Son carpetas referentes a todoa la docuemntacion que fue generad por la parte administrativa del sepdep	Información	Dirección Administrativa Financiera	Activos Fijos y Almacenes	Encargado de Activos Fijos y Almacenes	Encargado de Activos Fijos y Alamacenes	ALTO	MUY ALTO	BAJO	3.67	2023-09-01	2024-09-01

Evaluación del Riesgo

El responsable del activo de información determina; en base a sucesos, y la importancia que tiene el activo sobre las posibles amenazas y vulnerabilidades a las que está expuesto y realiza una descripción del escenario en el cual se puede dar la materialización de la amenaza, asumiendo que el responsable conoce y entiende los riesgos sobre el activo.La entidad o institución pública

Una vulnerabilidad es toda aquella debilidad que presenta el activo de información, dada comúnmente por la inexistencia o ineficacia de un control.

Una amenaza es todo elemento que haciendo uso o aprovechando una vulnerabilidad, atenta o puede atentar contra la seguridad de un activo de información. Las amenazas surgen a partir de la existencia de vulnerabilidades, independientemente de que se comprometa o no la seguridad de un sistema.

Evaluación del Riesgo la metodología seleccionada realiza la identificación, análisis y valoración de los riesgos asociados a los activos de información previamente identificados, clasificados y valorados y permite identificar amenazas y vulnerabilidades.

La Identificación del Riesgo se toma en cuenta las vulnerabilidades y amenazas que inciden en la confidencialidad, integridad y disponibilidad de la información.

Análisis y Valoración del Riesgo evalúa las posibles consecuencias de la materialización de una amenaza producto de las vulnerabilidades presentes en los activos de información.

La priorización esta claramente establecida a partir del nivel de riesgo máximo definido previamente por la entidad o institución pública a través del CSI.

Prioritarios

#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de riesgo
1	Equipos de computación	Virus infromatico	Ingresan Memorias USB que contienen virus	Falta de control de accesos	Muy Probable	Moderado	ALTO
2	Sistema Informático SISEC v3	Registro de dato erróneos	Usuario del sistema registra Datos incorrectos.	Falta de cuidado en la revisión de los datos	Probable	Moderado	MEDIO
3	Storage	Avería de origen físico o lógico	Falla del equipo por ausencia de mantenimientos preventivos	Ausencia de un eficiente control de mantenimiento	Muy Probable	Severo	ALTO
4	Correo Institucional	Ataque de Fuerza bruta	el atacante prueba sistemáticamente todas las combinaciones posibles de caracteres hasta que encuentra las credenciales correctas que le permitirán acceder al sistema o cuenta de destino.	Falta de uso de Activacion de autenticación de dos factores, Limitar los intentos de inicio de sesión, software actualizado o medidas de seguridad en el firewall	Probable	Severo	ALTO
5	UPS	Corte del suministro eléctrico	El equipo no funcione de forma adecuada ante la	Ausencia de cambio de baterías o UPS	Probable	Crítico	ALTO
6	Archivo del SEPDEP	perdida de documentacion	No existe un responsable que se haga cargo de la documentación archivada, lo que ocasiona perdida o alteración de documentos	falta de un control de documentación guardada	Poco Probable	Severo	MEDIO

No prioritarios

#	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de riesgo
7	Equipos de computación	Falla de Hardware	Altas temperaturas, altas tensiones de energía eléctrica, Polvo acumulado.	Falta de mantenimiento preventivo y oportuno	Poco Probable	Moderado	BAJO
8	Equipos Biometricos	Perdida de Informacion	Falla física de los equipos biométricos	Falta de renovación de equipos biométricos que tienen muchos años en funcionamiento	Probable	Menor	BAJO

Matriz de Valoración del Riesgo

Cierta/Inminente	BAJO	MEDIO	ALTO	CRÍTICO	CRÍTICO
Muy Probable	BAJO	MEDIO	ALTO 1, 9	ALTO 3, 11	CRÍTICO
Probable	IRRELEVANTE	BAJO 8, 16	MEDIO 2, 10	ALTO 4, 12	ALTO 5, 13
Poco Probable	IRRELEVANTE	BAJO	BAJO 7, 15	MEDIO 6, 14	MEDIO
Improbable	IRRELEVANTE	IRRELEVANTE	IRRELEVANTE	BAJO	BAJO
	Irrelevante	**Menor**	**Moderado**	**Severo**	**Crítico**

Tratamiento de Riesgo

Se tomarón decisiones acerca de las medidas más apropiadas para el tratamiento del riesgo identificado.

El tratamiento del riesgo implica tomar decisiones para aceptar, reducir, retener, evitar o transferir los riesgos.

Nro	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo	Control
1	Equipos de computación	Virus infromatico	Ingresan Memorias USB que contienen virus	Falta de control de accesos	Muy Probable	Moderado	ALTO	3.2.1.viii. Habilitar las cuentas de acceso basado en roles de usuario para el procesamiento, administración, consulta o uso de la información
2	Sistema Informático SISEC v3	Registro de dato erróneos	Usuario del sistema registra Datos incorrectos.	Falta de cuidado en la revisión de los datos	Probable	Moderado	MEDIO	3.2.2.ii. Se deberá dejar constancia sobre la aceptación del servidor público para el uso responsable de la información de accesos. 3.2.2.vii. El usuario propietario de la cuenta de acceso es responsable del uso de la contraseña.
3	Storage	Avería de origen físico o lógico	Falla del equipo por ausencia de mantenimientos preventivos	Ausencia de un eficiente control de mantenimiento	Muy Probable	Severo	ALTO	5.3.1.xvi. Se deberán programar mantenimientos periódicos del equipamiento del CPD.
4	Equipos Biometricos	Perdida de Informacion	Falla física de los equipos biométricos	Falta de renovación de equipos biométricos que tienen muchos años en funcionamiento	Probable	Moderado	MEDIO	8.2.1.iv. Debe obtenerse en la medida de lo posible, información oportuna de las vulnerabilidades técnicas de los sistemas, software y aplicaciones a ser adquiridos de terceros, así como la información relevante con respecto a actualizaciones y parches.
5	Correo Institucional	Ataque de Fuerza bruta	el atacante prueba sistemáticamente todas las combinaciones posibles de caracteres hasta que encuentra las credenciales correctas que le permitirán acceder al sistema o cuenta de destino.	Falta de uso de Activacion de autenticación de dos factores, Limitar los intentos de inicio de sesión, software actualizado o medidas de seguridad en el firewall	Probable	Severo	ALTO	7.2.1.vii. Utilizar protocolos y puertos seguros para la configuración del servicio de correo electrónico. 7.2.1.viii. Gestionar regularmente el almacenamiento de correo electrónico basura. 7.2.1.x. Se deberá instalar software anti-spam.
6	UPS	Corte del suministro eléctrico	El equipo no funcione de forma adecuada ante la	Ausencia de cambio de baterías o UPS	Probable	Crítico	ALTO	5.3.1.xiv. El suministro eléctrico al equipamiento del CPD deberá estar regulado y cumplir con las especificaciones técnicas. 5.3.1.xv. De acuerdo a requerimientos de disponibilidad, se deberá implementar suministro alterno de energía eléctrica y/o banco de baterías.

Nro	Activo	Amenaza	Situación	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo	Control
7	Archivo del SEPDEP	perdida de documentacion	No existe un responsable que se haga cargo de la documentación archivada, lo que ocasiona perdida o alteración de documentos	falta de un control de documentación guardada	Poco Probable	Severo	MEDIO	2.1.2.i. Identificar a los responsables y/o custodios de activos de información. 2.1.2.ii. Documentar el proceso de asignación y devolución de los activos de información a propietarios y/o custodios.

Listado de Controles Implementados y por Implementar

Control	SI/NO	Justificación
3.2.1.viii. Habilitar las cuentas de acceso basado en roles de usuario para el procesamiento, administración, consulta o uso de la información	si	
3.2.2.ii. Se deberá dejar constancia sobre la aceptación del servidor público para el uso responsable de la información de accesos.	si	
3.2.2.vii. El usuario propietario de la cuenta de acceso es responsable del uso de la contraseña.	si	
5.3.1.xvi. Se deberán programar mantenimientos periódicos del equipamiento del CPD.	si	
8.2.1.iv. Debe obtenerse en la medida de lo posible, información oportuna de las vulnerabilidades técnicas de los sistemas, software y aplicaciones a ser adquiridos de terceros, así como la información relevante con respecto a actualizaciones y parches.	si	
7.2.1.vii. Utilizar protocolos y puertos seguros para la configuración del servicio de correo electrónico.	si	
7.2.1.viii. Gestionar regularmente el almacenamiento de correo electrónico basura.	si	
7.2.1.x. Se deberá instalar software anti-spam.	si	
5.3.1.xiv. El suministro eléctrico al equipamiento del CPD deberá estar regulado y cumplir con las especificaciones técnicas.	si	
5.3.1.xv. De acuerdo a requerimientos de disponibilidad, se deberá implementar suministro alterno de energía eléctrica y/o banco de baterías.	si	
2.1.2.i. Identificar a los responsables y/o custodios de activos de información.	si	
2.1.2.ii. Documentar el proceso de asignación y devolución de los activos de información a propietarios y/o custodios.	si	

Controles Implementados y por Implementar

Directriz				
2.1.2.i. Identificar a los responsables y/o custodios de activos de información.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivo del SEPDEP	MEDIO	perdida de documentacion	No existe un responsable que se haga cargo de la documentación archivada, lo que ocasiona perdida o alteración de documentos	falta de un control de documentación guardada
Desarrollo				
Se debe nombrar a las personas responsables del archivo				

Directriz				
2.1.2.ii. Documentar el proceso de asignación y devolución de los activos de información a propietarios y/o custodios.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Archivo del SEPDEP	MEDIO	perdida de documentacion	No existe un responsable que se haga cargo de la documentación archivada, lo que ocasiona perdida o alteración de documentos	falta de un control de documentación guardada
Desarrollo				
el responsable debe registrar a los funcionarios que estan utilizando los archivos				

Directriz				
3.2.1.viii. Habilitar las cuentas de acceso basado en roles de usuario para el procesamiento, administración, consulta o uso de la información				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Equipos de computación	ALTO	Virus infromatico	Ingresan Memorias USB que contienen virus	Falta de control de accesos
Desarrollo				
Se estableceran usuarios diferentes en las computadoras limitando accesos a diferentes funcionalidades				

Directriz				
3.2.2.ii. Se deberá dejar constancia sobre la aceptación del servidor público para el uso responsable de la información de accesos.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Sistema Informático SISEC v3	MEDIO	Registro de dato erróneos	Usuario del sistema registra Datos incorrectos.	Falta de cuidado en la revisión de los datos
Desarrollo				
Se requiere informar a los funcionarios publicos las condiciones de uso del sistema SISEC V3				

Directriz				
3.2.2.vii. El usuario propietario de la cuenta de acceso es responsable del uso de la contraseña.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Sistema Informático SISEC v3	MEDIO	Registro de dato erróneos	Usuario del sistema registra Datos incorrectos.	Falta de cuidado en la revisión de los datos
Desarrollo				
Se debe realizara capacitaciones constantes para concientizar sibre el uso de contraseñas seguras y el cambio periodico				

Directriz				
5.3.1.xiv. El suministro eléctrico al equipamiento del CPD deberá estar regulado y cumplir con las especificaciones técnicas.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**

Directriz				
UPS	ALTO	Corte del suministro eléctrico	El equipo no funcione de forma adecuada ante la	Ausencia de cambio de baterías o UPS
Desarrollo				
Se debe realizar las especificaciones tecnivas del UPS acorde a las necesidades de la entidad				

Directriz				
5.3.1.xv. De acuerdo a requerimientos de disponibilidad, se deberá implementar suministro alterno de energía eléctrica y/o banco de baterías.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
UPS	ALTO	Corte del suministro eléctrico	El equipo no funcione de forma adecuada ante la	Ausencia de cambio de baterías o UPS
Desarrollo				
Se gestionara la adquiscion de un UPS				

Directriz				
5.3.1.xvi. Se deberán programar mantenimientos periódicos del equipamiento del CPD.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Storage	ALTO	Avería de origen físico o lógico	Falla del equipo por ausencia de mantenimientos preventivos	Ausencia de un eficiente control de mantenimiento
Desarrollo				
Se realizaran mantenimientos al CPD de forma semestral				

Directriz				
7.2.1.vii. Utilizar protocolos y puertos seguros para la configuración del servicio de correo electrónico.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Correo Institucional	ALTO	Ataque de Fuerza bruta	el atacante prueba sistemáticamente todas las combinaciones posibles de caracteres hasta que encuentra las credenciales correctas que le permitirán acceder al sistema o cuenta de destino.	Falta de uso de Activacion de autenticación de dos factores, Limitar los intentos de inicio de sesión, software actualizado o medidas de seguridad en el firewall
Desarrollo				
Se requiere la reconfiguracion del sistema de corresos institucionales				

Directriz				
7.2.1.viii. Gestionar regularmente el almacenamiento de correo electrónico basura.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Correo Institucional	ALTO	Ataque de Fuerza bruta	el atacante prueba sistemáticamente todas las combinaciones posibles de caracteres hasta que encuentra las credenciales correctas que le permitirán acceder al sistema o cuenta de destino.	Falta de uso de Activacion de autenticación de dos factores, Limitar los intentos de inicio de sesión, software actualizado o medidas de seguridad en el firewall
Desarrollo				
Se requiere realizar mantenimientos periodicos a la informacion entrante y saliente				

Directriz				
7.2.1.x. Se deberá instalar software anti-spam.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**

Directriz				
Correo Institucional	ALTO	Ataque de Fuerza bruta	el atacante prueba sistemáticamente todas las combinaciones posibles de caracteres hasta que encuentra las credenciales correctas que le permitirán acceder al sistema o cuenta de destino.	Falta de uso de Activacion de autenticación de dos factores, Limitar los intentos de inicio de sesión, software actualizado o medidas de seguridad en el firewall
Desarrollo				
Se gestionara la adquiscion de un firewall con antispam o el servicio correspondiente				

Directriz				
8.2.1.iv. Debe obtenerse en la medida de lo posible, información oportuna de las vulnerabilidades técnicas de los sistemas, software y aplicaciones a ser adquiridos de terceros, así como la información relevante con respecto a actualizaciones y parches.				
Activo	**Riesgo**	**Amenaza**	**Situación**	**Vulnerabilidad**
Equipos Biometricos	MEDIO	Perdida de Informacion	Falla física de los equipos biométricos	Falta de renovación de equipos biométricos que tienen muchos años en funcionamiento
Desarrollo				
Se deberá obtener información de los años de vida útil de los biométricos para solicitar la compra de nuevo equipamiento o mantenimiento				

Controles Mínimos de Seguridad de la Información

Los controles de Seguridad de la información que seran implementados se encuentran referenciados en "Controles Implementados y por Implementar" y en el punto de "Desarrollo" de la politica de la Seguridad de la Información y sus respectivos archivos adjuntos

Indicadores y Métricas

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

En general, un indicador y métrica deberá ser:

a) Específico.

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

c) Alcanzable.

d) Relevante.

e) Repetible en periodos de tiempo.

2023

#	Control de Seguridad	Indicador y métrica	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	8. Desarrollo, mantenimiento y adquisición de sistemas													
		Se debera tener respaldo de la informacion de los equipos instalados en el sepdep como tiempo de vida, mantenimiento y otros									Ini: 1			
2	3. Control de accesos													
		Captura de pantallas de "politicas de uso" aceptadas en el sistema de seguimiento de casos									Ini: 1			
		Circular del uso de contraseñas									Ini: 1			
2	2. Gestión de activos de información													
		Reglamento realizado para el uso de medios de almacenamiento removibles									Ini: 1			
2	5. Seguridad física y ambiental													
		Numero de informes de mantenimiento al CPD									Ini: 1			
2	7. Seguridad de las comunicaciones													
		informe de configuracion del servidos de correos institucionales									Ini: 1			

2024

#	Control de Seguridad	Indicador y métrica	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	8. Desarrollo, mantenimiento													

#	Control de Seguridad	Indicador y métrica	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
	y adquisición de sistemas													
		Se debera tener respaldo de la informacion de los equipos instalados en el sepdep como tiempo de vida, mantenimiento y otros									Fin: 2			
2	3. Control de accesos													
		Captura de pantallas de "politicas de uso" aceptadas en el sistema de seguimiento de casos									Fin: 2			
		Circular del uso de contraseñas									Fin: 2			
2	2. Gestión de activos de información													
		Reglamento realizado para el uso de medios de almacenamiento removibles									Fin: 1			
2	5. Seguridad física y ambiental													
		Numero de informes de mantenimiento al CPD									Fin: 1			
2	7. Seguridad de las comunicaciones													
		informe de configuracion del servidos de correos institucionales									Fin: 1			

Cronograma de Implementación

En el marco del Plan Institucional de Seguridad de la Información, la entidad o institución pública elabora un cronograma de implementación de los controles definidos. Para esto, todos los procesos y/o procedimientos que se desprenden de la Política de Seguridad de la Información ya se encuentran elaborados para su aplicación. El cronograma de implementación contempla mínimamente:

a) Fechas.

b) Controles a implementarse.

c) Roles y responsabilidades.

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

2023

#	Control de Seguridad	Actividad	Roles y Responsabilidades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	8. Desarrollo, mantenimiento y adquisición de sistemas														
		se realizara la obtencion de	RSI, CSI								Ini: 1				

#	Control de Seguridad	Actividad	Roles y Responsabilidades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
		informacion de los equipos de computacion para planes de contingencia													
2	3. Control de accesos														
		Se desarrollará la página para las políticas de uso y se realizará la capacitación correspondiente	RSI, CSI .								Ini: 1				
2	2. Gestión de activos de información														
		se realizara un procedimientos para el uso de medios de almacenamiento removibles	RSI y CSI								Ini: 1				
2	5. Seguridad física y ambiental														
		Se realizaran dos mantenimientos al área de servidores y se gestionara la adquisición de equipamiento si corresponde	RSI y CSI								Ini: 1				
2	7. Seguridad de las comunicaciones														
		Se gestionara la reconfiguracion del servidor de correos institucionales y su mantenimientos correspondiente	RSI y CSI								Ini: 1				

2024

#	Control de Seguridad	Actividad	Roles y Responsabilidades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	8. Desarrollo, mantenimiento y adquisición de sistemas														
		se realizara la obtencion de informacion de los equipos de computacion para planes de contingencia	RSI, CSI								Fin: 1				
2	3. Control de														

#	Control de Seguridad	Actividad	Roles y Responsabilidades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
	accesos														
		Se desarrollará la página para las políticas de uso y se realizará la capacitación correspondiente	RSI, CSI .								Fin: 1				
2	2. Gestión de activos de información														
		se realizara un procedimientos para el uso de medios de almacenamiento removibles	RSI y CSI								Fin: 1				
2	5. Seguridad física y ambiental														
		Se realizaran dos mantenimientos al área de servidores y se gestionara la adquisición de equipamiento si corresponde	RSI y CSI								Fin: 1				
2	7. Seguridad de las comunicaciones														
		Se gestionara la reconfiguracion del servidor de correos institucionales y su mantenimientos correspondiente	RSI y CSI								Fin: 1				

Historial de Cambios

Fecha	Formulario	Estado	Encargado
2023-08-30	Etapa Inicial	EN_REVISION	Octavio Jesús Torrico Álvarez
2023-08-30	Etapa Inicial	APROBADO	Comite seguridad de la informacion
2023-08-31	Gestión de Riesgos	EN_REVISION	Octavio Jesús Torrico Álvarez
2023-08-31	Gestión de Riesgos	APROBADO	Comite seguridad de la informacion
2023-08-31	Políticas de Seguridad	EN_REVISION	Octavio Jesús Torrico Álvarez
2023-08-31	Políticas de Seguridad	APROBADO	Comite seguridad de la informacion
2023-08-31	Tratamiento de Riesgo	EN_REVISION	Octavio Jesús Torrico Álvarez
2023-08-31	Tratamiento de Riesgo	APROBADO	Comite seguridad de la informacion
2023-08-31	Indicadores y Metricas	EN_REVISION	Octavio Jesús Torrico Álvarez
2023-08-31	Indicadores y Metricas	APROBADO	Comite seguridad de la informacion
2023-08-31	Controles implementados y por implementar	EN_REVISION	Octavio Jesús Torrico Álvarez
2023-08-31	Controles implementados y por implementar	APROBADO	Comite seguridad de la informacion

ANEXO

Documentación de la Entidad

En esta etapa, el Responsable de Seguridad de la Información identifico las siguientes fuentes principales de insumo para elaborar el PISI, que son listadas a continuación:

Para la elaboración del presente Plan se tiene como base documental y fuentes principales de insumos la siguiente documentación institucional:

- Plan Operativo Anual - POA 2023.
- Plan Estratégico Institucional - PEI 2021- 2025.
- Plan de Gobierno Electrónico Institucional del SEPDEP– PGE.
- Plan Institucional de Software Libre y Estándares Abiertos del SEPDEP – PISLEA.
- Reglamento Interno de Personal – RIP y la normativa que se desprende del mismo.
- Contratos con Proveedores Externos (Servicios de Internet, telefonía, mantenimiento entre otros)

Responsabilidades de la Máxima Autoridad Ejecutiva

La Máxima Autoridad Ejecutiva deberá:

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

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

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

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

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

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

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

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

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

Lo cual se puede evidenciar en el documento adjunto:

Responsabilidades de la Máxima Autoridad Ejecutiva.pdf,

Documento de Designación y Funciones del Responsable de Seguridad de la Información

El RSI tendrá las siguientes funciones:

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

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

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

d) Gestionar el cumplimiento del PISI.

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

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

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

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

i) Coadyuvar en la gestión de contingencias tecnológicas.

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

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

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

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

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

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

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

Lo cual se puede evidenciar en el documento adjunto, donde ademas se cuenta con la designación del RSI en una nota firmada por MAE:

RSI.pdf,

Documento de Conformación y Funciones del Comité de Seguridad de la Información

Mediante resolución expresa, la Máxima Autoridad Ejecutiva designa al personal que conformará el Comité de Seguridad de la Información (CSI).

El CSI esta conformado por:

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

b) Personal de nivel jerárquico, de acuerdo a la estructura organizativa de la entidad o institución pública. (detalle de quienes forman parte del Comité)

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

El CSI establece su organización interna y 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 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.

Lo cual se puede evidenciar con la Resolución Administrativa y los documentos que se encuentran adjuntos a continuación

RESOLUCION 30-2023.pdf,

Definición del Alcance del PISI

En Reunión del Comite de Seguridad de la Información define el alcance del PISI como:

El Plan Institucional de Seguridad de la Información tiene como alcance:
Coadyuvar con el Plan Estratégico Institucional - PEI 2021-2025, en sus dos (2) objetivos estratégicos institucionales los cuales son:

Objetivo Estratégico 1: Se ha fortalecido la capacidad institucional del SEPDEP mediante una gestión transparente, eficiente y efectiva en beneficio de los usuarios

Objetivo Estratégico 2: Garantizar que es el SEPDEP preste un servicio gratuito de defensa técnica en procesos penales, a todo imputado carente de recursos, precautelando sus derechos y garantías, conforme establece la Constitución Política del Estado, así como tratados y convenios internacionales.