BICENTENARIO DE BOLIVIA

ESTADO PLURINACIONAL DE BOLIVIA

MINISTERIO DE OBRAS PÚBLICAS, SERVICIOS Y VIVIENDA

ESTADO PLURINACIONAL DE
BOLIVIA

MINISTERIO DE OBRAS PÚBLICAS, SERVICIOS Y VIVIENDA

DIRECCIÓN GENERAL DE ASUNTOS ADMINISTRATIVOS

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI)

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Aprobado por Resolución Ministerial N° 232

De Fecha: 26 NOV. 2024

D.G.A.A. - U.A. Vobo Mariela Ventura C. M.O.P.S.

D.G.A.A. - U.A. Vobo Mariela Ventura C. M.O.P.S.

D.G.A.A. - U.A. Vobo Jaime Panzi M.O.P.S.V.

La Paz – Bolivia

Contenido

D.G.A.A. - U.A. V°B° Ivet Mariño M.O.P.S.V.

D.G.A.A. - U.A. V°B° Marco A. Ventura C. M.O.P.S.V.

D.G.A.A. - U.A. V°B° Sonia Patzi M.O.P.S.V.

PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

I. CAPÍTULO I.- GENERALIDADES

1. INTRODUCCIÓN

El Ministerio de Obras Publicas Servicios y Vivienda determina la información como un activo de alta importancia para la entidad que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información. El documento establece las políticas que integran el Plan Institucional de Seguridad de la Información PISI, las cuales deben ser adoptadas por los funcionarios, consultores, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el MOPSV; estas se encuentran enfocadas al cumplimiento de la normatividad legal boliviana vigente y a las buenas prácticas de seguridad de la información. La seguridad de la información es para el MOPSV, una labor prioritaria que exhorta a todos a velar por el cumplimiento de las políticas establecidas en el presente documento.

2. ANTECEDENTES

El Ministerio de Obras Públicas, Servicios y Vivienda (MOPSV), como entidad del sector público en aplicación de la Ley 1178 de 20 de junio de 1990, Ley de Administración y Control Gubernamentales (SAFCO), en función de sus objetivos y la naturaleza de sus actividades, debe implementar, los sistemas de administración y control.

El Decreto Supremo 23318-A de 3 de noviembre de 1992, Decreto Supremo N° 26237, de 29 de junio de 2001 modificatorio al Reglamento de la Responsabilidad por la Función Pública que determina entre otros, los conceptos de eficacia, economía, eficiencia, desempeño transparente de funciones, la finalidad, atribuciones, funciones, facultades y deberes, aplicables a la gestión pública, de igual manera se establece la línea de mando por el cual todo servidor público debe responder ante sus superiores jerárquicos.

El Decreto Supremo N° 4857 de 06 de enero de 2023, consolida la estructura jerárquica del Ministerio de Obras Públicas, Servicios y Vivienda es la siguiente:

MINISTRA (O) DE OBRAS PÚBLICAS, SERVICIOS Y VIVIENDA

- Viceministerio de Transportes
  - ✓ Dirección General de Transporte Terrestre, Fluvial y Lacustre
  - ✓ Dirección General de Transporte Aéreo
- Viceministerio de Telecomunicaciones
  - ✓ Dirección General de Telecomunicaciones
  - ✓ Dirección General de Servicios en Telecomunicaciones
- Viceministerio de Vivienda y Urbanismo
  - ✓ Dirección General de Vivienda y Urbanismo

- ✓ Dirección General de Ordenamiento Urbano

2.1. 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:

Las fuentes principales para la elaboración del PISI son el Plan Estratégico Institucional - PEI 2021- 2025 en base al enfoque político de la entidad, las atribuciones y competencias, misión, visión, principios, valores, estado de situación actual, matriz toda, objetivos y estrategias institucionales.

2.1.1.Misión

Promover y gestionar el acceso universal y equitativo de la población boliviana a obras y servicios de calidad, en telecomunicaciones, transportes y vivienda, en armonía con la naturaleza

2.1.2.Visión

Somos una entidad que, con calidad y transparencia, satisface las necesidades de transportes, telecomunicaciones y vivienda de la población boliviana.

2.1.3.PLAN ESTRATÉGICO

El Plan Estratégico Institucional (PEI), fue aprobado mediante Resolución Ministerial N° 134, de fecha 20 de julio de 2022, está en función a los objetivos estratégicos del MOPSV. En este sentido, el MOPSV ha definido su Enfoque Político de la siguiente forma.

2.1.3.1. MARCO ESTRATEGICO

Registrar la articulación del PDES – PSDI – PEI – POA (acciones de corto plazo) de acuerdo al siguiente:

PLAN	CODIGO		DETALLE
PLAN GENERAL DE DESARROLLO ECONOMICO Y SOCIAL (PGES 2016-2025), AGENDA PATRIOTICA	**Pilar**	**11**	Soberanía y transparencia en la gestión pública bajo los principios de no robar, no mentir y no ser flojo.
PLAN DE DESARROLLOECONOMICO Y SOCIAL (PDES 2021-2025)	**Eje**	**7**	Reforma Judicial, Gestión Publica Digitalizada y transparente Seguridad y Defensa Integral con Soberanía Nacional.
	Meta	**7.1**	Impulsar el acceso a la justicia social y reparadora para todas y todos sobre la base de la reforma del Sistema Judicial y de una gestión pública transparente que lucha frontalmente contra la corrupción.
	Resultado	**7.1.7**	Se ha fortalecido la gestión pública para el ejercicio democrático e institucional del estado, conforme a las necesidades del pueblo boliviano fortaleciendo el acceso a la información y comunicación

	Acción	**7.1.7.1**	Gestión pública a través de acciones de coordinación, apoyo institucional, seguimiento y evaluación
PLAN SECTORIAL DE DESARROLLO INTEGRAL PARA EL VIVIR BIEN (PSDI 2021-2025)	**Resultado (Impacto Sectorial)**	**7.1.7.1.1**	Transportes Telecomunicaciones y Tecnologías de Información y Comunicación Hábitat y Vivienda.
PLAN ESTRATEGICO INSTITUCIONAL DEL MOPSV	**Objetivo Estratégico Institucional (impacto institucional)**	**7.1.7.1.1.1**	Fortalecer y coadyuvar la gestión administrativa para contribuir a los Objetivos Estratégicos Institucionales de manera eficaz, transparente, oportuna en la administración de bienes, servicios y normas.
	Acciones de Mediano Plazo (Acción Estratégica Institucional)	**7.1.7.1.1.1.1**	Realizar acciones de coordinación, apoyo institucional, seguimiento y evaluación a las áreas organizacionales sustantivas, administrativas y de asesoramiento para contribuir a los Objetivos Estratégicos Institucionales.
PROGRAMA OPERATIVO ANUAL (POA) 2023	**Acción de Corto Plazo**	**7.1.7.1.1.1.1.1**	Coordinar y asesorar una gestión administrativa, financiera, jurídica, comunicacional e institucional de forma eficaz y eficiente.

2.1.3.2. OBJETIVO ESTRATÉGICO INSTITUCIONAL

	OBJETIVO ESTRATÉGICO INSTITUCIONAL	ESTRATEGIA INSTITUCIONAL
GESTIÓN ADMINISTRATIVA	Fortalecer y coadyuvar la gestión administrativa para contribuir a los Objetivos Estratégicos Institucionales de manera eficaz, transparente, oportuna en la administración de bienes, servicios y normas	Fortalecimiento de la gestión Pública, a través de una adecuada gestión de recursos administrativos, financieros, normativos, con transparencia y de manera oportuna, efectuando seguimiento y evaluación a la programación y ejecución de acciones estratégicas, además de brindar asesoramiento a los Viceministerios y Entidades bajo tuición, en el marco de las atribuciones del Ministerio de Obras Públicas, Servicios y Vivienda.
VICEMINISTERIO DE TRANSPORTES	Mejorar la prestación de servicios de transporte terrestre	Efectuar la recaudación por la prestación de servicios a operadores.
	Mejorar y aumentar la infraestructura y equipamiento del transporte aéreo para contribuir al desarrollo e integración de los bolivianos a fin de generar mejores condiciones socio productivas.	Promover y desarrollar proyectos de inversión que contribuyan al transporte aéreo.
	Mejorar los servicios de transporte aéreo para la integración del país.	Promover el desarrollo del transporte aéreo Realizar actividades referidas al cese de operaciones y liquidación de AASANA.
	Mejorar y aumentar la infraestructura y equipamiento del transporte ferroviario para contribuir al desarrollo e integración de los bolivianos a fin de generar mejores condiciones socio productivas	Promover y desarrollar proyectos de inversión que contribuyan al fortalecimiento del transporte ferroviario. Así como, el fortalecimiento institucional del Sistema Ferroviario.
	Mejorar y aumentar la infraestructura y equipamiento del transporte fluvial y lacustre para contribuir al desarrollo e integración de los bolivianos a fin de generar mejores condiciones socio productivas	Promover y desarrollar las rutas fluviales, infraestructura portuaria para el transporte de bienes y servicios.
	Mejorar y aumentar la infraestructura y equipamiento del transporte urbano para contribuir al desarrollo e integración de los bolivianos a fin de generar mejores condiciones socio productivas.	Promover y desarrollar proyectos de inversión que contribuyan al transporte urbano.
	Implementar normativa y proyectos para el desarrollo de la logística	Promover normativa y proyectos para el desarrollo de la logística. Así como, el fortalecimiento institucional que contribuyan a la logística.
	Implementar políticas públicas del sector de transportes	Promover normativa y proyectos para el desarrollo del sector transportes, en sus diferentes modalidades. Así como el fortalecimiento institucional que contribuyan al sector
VICEMINISTERIO DE	Coadyuvar a incrementar del 81% al 100% la tasa de cobertura de localidades con población mayor a 50	Alcanzar la universalización de las telecomunicaciones aprovechando la predisposición de la sociedad a la adopción y utilización de servicios de telecomunicaciones

TELECOMUNICACIONES	habitantes, con servicio de telefonía móvil y/o acceso a Internet.	Aprovechar la oferta de recursos de organismos multilaterales y de cooperación para el financiamiento de proyectos de expansión de redes de telecomunicaciones Aprovechar la capacidad en la elaboración de proyectos de expansión de redes de telecomunicaciones para gestionar recursos ante organismos nacionales e internaciones ante la posible reducción de recursos económicos Alcanzar la universalización de las telecomunicaciones aprovechando la predisposición de la sociedad a la adopción y utilización de servicios de telecomunicaciones Elaborar e implementar normativa que coadyuve a dar celeridad a los requerimientos del VMTEL realizados a las entidades ejecutoras de los recursos PRONTIS Aprovechar la capacidad de respuesta a requerimientos sectoriales para dar solución a los solicitudes de las organizaciones sociales. Aprovechar el marco normativo constitucional favorable para elaborar e implementar normativa orientada al uso de los recursos del sector en proyectos de acceso universal Aprovechar la oferta de recursos de organismos multilaterales y de cooperación para gestionar recursos orientados al cumplimiento de los objetivos sectoriales Desarrollar e implementar políticas y estrategias de coordinación con entidades territoriales autónomas para la implementación de proyectos de telecomunicaciones y TIC en el área rural Aprovechar la precisión social para gestionar que los recursos generados por el sector sean utilizados en su totalidad en proyectos de acceso universal Aprovechar la precisión social para gestionar con celeridad la reposición de los cargos vacantes
	Coadyuvar a Implementar 3 Centros Tecnológicos o Ciudadelas del Conocimiento	Implementar proyectos de innovación tecnológica en Telecomunicaciones y TIC para el sector productivo Implementar políticas, normativa, planes, programas y proyectos del sector Telecomunicaciones y TIC, ante la creciente demanda por servicios de telecomunicaciones Desarrollar e implantar un sistema integrado de información con financiamiento interno o externo, aprovechando las relaciones institucionales nacionales e internacionales del sector Elaborar e implementar políticas, estrategias, planes y normativa de innovación y desarrollo que contrarreste una posible crisis económica y financiera Utilizar las nuevas tecnologías del sector telecomunicaciones y TIC en la gestión administrativa del Viceministerio de Telecomunicaciones
	Coadyuvar a mantener actualizada al 100% las políticas, planes y normativa del sector programadas para el periodo	Desarrollar e implementar políticas y estrategias de coordinación interna e intersectorial para satisfacer la creciente demanda de servicios en Telecomunicaciones y TIC Aprovechar las relaciones con instituciones internacionales del sector para incrementar la participación en instancias internacionales de los sectores telecomunicaciones, TIC y postal Elaborar e implementar normativa en coordinación con las entidades territoriales autónomas para mejorar la atención a demandas en telecomunicaciones y TIC de su competencia Elaborar e implementar normativa para satisfacer la creciente demanda por servicios de telecomunicaciones y TIC Aprovechar el marco normativo constitucional favorable para elaborar e implementar normativa enfocada al desarrollo del sector Utilizar las nuevas tecnologías del sector telecomunicaciones y TIC en la gestión administrativa el Viceministerio de Telecomunicaciones

		Coordinar con las entidades gubernamentales relacionadas con el sector o proyectos sociales del sector para la elaboración de normativa de telecomunicaciones y TIC que beneficie al sector
		Realizar el rediseño organizacional orientado a cumplir con el acelerado desarrollo de las telecomunicaciones y TIC
		Aprovechar la asistencia técnica de organismos internacionales para elaborar planes, programas y proyectos de telecomunicaciones y TIC que involucren la participación de otros ministerios y entidades en el ámbito de las TIC dependientes de otras Carteras de Estado
		Aprovechar el ser cabeza de un sector de permanente innovación y desarrollo para la elaboración y ejecución de proyectos que utilicen nuevas tecnologías para el sector de Telecomunicaciones y TIC
	Coadyuvar a Implementar proyectos para el desarrollo integral del Sector Telecomunicaciones y Tecnologías de Información y Comunicación	Impulsar el desarrollo de la innovación tecnológica en coordinación con entidades gubernamentales relacionadas con el sector
		Mejorar la celeridad de los procesos administrativos internos e interministeriales mediante la elaboración y aplicaciones de instrumentos de control interno como los manuales de procesos y procedimientos
	Coadyuvar a Gestionar la ejecución de proyectos y acciones para la universalización de las telecomunicaciones	Mejorar la celeridad de los procesos administrativos internos e interministeriales mediante la elaboración y aplicaciones de instrumentos de control interno como los manuales de procesos y procedimientos
	Fortalecer los mecanismos de regularización de predios urbanos, mediante procesos administrativos y judiciales a través de lo establecido en la LEY N° 1227 DE MODIFICACIÓN DE LA LEY N° 247 MODIFICADO POR LA LEY N° 803 Y LA LEY N° 915 DE REGULARIZACIÓN DEL DERECHO PROPIETARIO SOBRE BIENES INMUEBLES URBANOS DESTINADOS A VIVIENDA	Efectuar el seguimiento a la regularización de predios urbanos mediante procesos administrativos y judiciales
	Concluir todas las tareas pendientes del ex FONVIS en Liquidación, a través del procesamiento de la documentación e información que permitan identificar los procesos judiciales, cartera a recuperar, saneamientos pendientes, minutaciones.	Finalizar las tareas pendientes de recuperación, minutación y conciliación del ex FONVIS e instituciones de vivienda.
	Mejoramiento y desarrollo del marco normativo, lineamientos estratégicos e instrumentos para la gestión e implementación de la Política Nacional de Vivienda	Contribuir y fortalecer a la normativa Nacional de Vivienda.
VICEMINISTERIO DE VIVIENDA Y URBANISMO	Mejoramiento y desarrollo del marco normativo para la aprobación de implementación de la Política Nacional de Desarrollo Integral de Ciudades	Contribuir y fortalecer los procesos de planificación urbana.
	Implementar la Política Nacional de Desarrollo Integral de Ciudades.	Realizar el diseño de los componentes operativos de la Política Nacional de Desarrollo Integral de Ciudades
	Fortalecer a los GAM's en la generación y administración de información urbana	Diseñar y elaborar sistemas de información urbana
	Gobiernos Autónomos Municipales con Catastros Urbanos en funcionamiento y actualizados con todos sus componentes que apoyan a la seguridad técnica y legal de la tenencia de la vivienda.	Implementar todos los componentes que apoyan a la seguridad técnica y legal de la tenencia de la vivienda.
	Contribuir a la planificación del desarrollo y gestión del suelo urbano	Diseñar el programa de desarrollo urbano
	Implementar el programa de desarrollo urbano	Elaborar y ejecutar un programa de desarrollo urbano
	Elaborar proyectos para el desarrollo urbano	Efectuar la gestión de proyectos para el desarrollo urbano
	Coordinar la formulación de un plan multisectorial	Mejorar las condiciones de acceso a oportunidades y recursos a sectores vulnerables
	Administrar los recursos de manera eficiente para el cumplimiento de resultados	Gestionar los recursos para el desarrollo del sector hábitat y vivienda

II. CAPÍTULO II.- ALCANCE DEL PLAN

En relación a las atribuciones del Ministerio de Obras Públicas, Servicios y Vivienda, el Comité de Tecnologías y Seguridad de la Información definió que el alcance para el presente plan, contemple a las áreas organizacionales de la entidad de carácter sustantivo y administrativo, dichas Unidades y/o áreas son:

MOPSV - Gestión Administrativa: Conformada por las Direcciones y Unidades Organizacionales transversales en la estructura del Ministerio:

Despacho

- Unidad de Auditoria Interna
- Unidad de Comunicación
- Unidad de Transparencia y Lucha contra la Corrupción
- Dirección General de Asuntos Administrativos: Unidad Administrativa, Unidad Financiera, Unidad de Recursos Humanos, Unidad de Desarrollo Tecnológico e Información.
- Dirección General de Asuntos Jurídicos: Unidad de Gestión Jurídica, Unidad de Análisis Jurídico.
- Dirección General de Planificación

Viceministerio de Telecomunicaciones: Conformada por las siguientes direcciones:

- Dirección General de Telecomunicaciones
- Dirección General de Servicios en Telecomunicaciones
  - Unidad de Ejecución de Proyectos del PRONTIS

Viceministerio de Transportes: Conformada por las siguientes direcciones:

- Dirección General de Transporte Aéreo
- Dirección General de Transporte Terrestre Fluvial y Lacustre
  - Unidad de Servicio a Operadores
  - Unidad de Gestión de Proyectos
  - Unidad Técnica de Hidrovias

Viceministerio de Vivienda y Urbanismo:

- Dirección General de Vivienda y Urbanismo
  - Unidad de Políticas de Vivienda
  - Unidad de Políticas de Desarrollo Urbano
- Dirección General de Ordenamiento Urbano

Unidades Ejecutoras:

- Unidad Ejecutora de titulación
- Unidad Ejecutora PROREVI
- Unidad Técnica de ferrocarriles
- Unidad Técnica Aeroportuaria

Asimismo, entiéndase que el efecto del presente documento, es de carácter global a toda la entidad en relación a la ejecución de actividades del plan, el cumplimiento de las políticas de seguridad de la información, entre otros.

D.G.A.A. - U.A. VºBº Marco A. Ventura C. M.O.P.S.V.

D.G.A.A. - U.A. VºBº Janina Penzi M.O.P.S.V.

DGAA - U.A. VºBº Iva Marello M.O.P.S.V.

1. OBJETIVO GENERAL

Establecer las políticas que regulan la seguridad de la información y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los funcionarios, consultores, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el MOPSV, mediante su centro de procesamiento de datos administrado por la Unidad de Desarrollo de Tecnologías de la Información.

2. OBJETIVOS ESPECÍFICOS

- Establecer los roles de las personas a cargo de esta tarea.
- Proponer controles para la protección.

3. ALCANCE

Aplica a todos los datos alojados en los servidores del centro de procesamiento de datos. Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, consultores y terceros que presten sus servicios o tengan algún tipo de relación con el MOPSV, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho documento. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por el Comité de Seguridad de la Información. Estas políticas como parte del Plan Institucional de Seguridad de la Información PISI, tiene alcance en todos los procesos que hacen parte del Centro de Procesamiento de Datos del Ministerio de Obras Publicas Servicios y Vivienda, además de poder ser actualizadas en el momento que así lo requiera el Responsable de Seguridad de la Información o el Comité de Seguridad de la Información.

El Comité de Seguridad de la Información en el presente documento establece que se tiene por alcance el Centro de Procesamiento de Datos del MOPSV, pudiendo en las siguientes versiones incluir otras unidades de la institución

4. ROLES Y RESPONSABILIDADES

Es responsabilidad de cada usuario aplicar las políticas de seguridad establecidas para la institución, conservar una copia de seguridad de todos sus archivos: Los usuarios son responsables por sus datos personales, como fotos, videos y archivos de música, ya sea que los mismos se encuentren en sus máquinas personales o en los servidores del MOPSV que se encuentren alojados en el Centro de Procesamiento de Datos a cargo de la UDTI.

De la misma manera, es responsabilidad del usuario mantener siempre en su computadora o en otro medio alternativo, una copia (copias de respaldo) de todos sus correos, archivos adjuntos, google docs., sites, calendars, etc. para poder reponerlos en caso de algún eventual problema en el servidor. La UDTI no realiza copias de seguridad de las cuentas de Google u otro medio externo al MOPSV, ya que las mismas son de carácter privado, y por otro lado no se cuenta con la infraestructura de almacenamiento suficiente para ello.

5. 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.	Se implementarán controles para la protección de la información institucional ante amenazas que se originan del recurso humano.	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.	Se implementarán controles para la protección de los activos ante amenazas que se originan.	Utiliza
3. Control de accesos Gestionar los accesos a servicios y aplicaciones que permitan controlar, autorizar y asignar privilegios a cuentas de usuario.	Se implementarán controles de accesos para la protección de la información institucional ante amenazas que se originan	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 autenticación.	Se implementarán controles criptográficos para la protección de la información institucional ante amenazas que se originan	Utiliza
5. Seguridad física y ambiental Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene información considerada sensible y critica para la entidad o institución pública, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información	Se implementarán controles para la protección física de la información institucional ante amenazas que se originan.	Utiliza
6. Seguridad de las operaciones Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta.	Se implementarán controles de las operaciones para la protección de la información institucional ante amenazas que se originan	Utiliza
7. Seguridad de las comunicaciones Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos.	Se implementarán controles para la protección de la información institucional ante amenazas que se originan en 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.	Se implementarán controles para la protección de la información institucional ante amenazas que se originan del desarrollo, mantenimiento y adquisición de sistemas	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.	Se implementarán controles para la protección de la información institucional ante amenazas que se originan de la gestión de incidentes de seguridad de la información.	Utiliza
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.	Se implementara plan de contingencias tecnológicas para la protección de la información institucional ante amenazas que se originan.	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.	Se implementarán controles para el cumplimiento de la protección de la información institucional ante amenazas que se originan.	Utiliza

6. APROBACIÓN Y VIGENCIA

El presente documento se aprueba por Resolución Ministerial del Ministerio de Obras Públicas, servicios y Vivienda MOPSV, en calidad de Máxima Instancia Ejecutiva y entrará en vigencia a partir de su aprobación.

7. ELABORACIÓN Y/O ACTUALIZACION

El Área de Normas en coordinación con las Áreas o/y Unidades Organizacionales, será responsable de la elaboración y/o actualización del presente documento en base a la experiencia de su aplicación o modificación normativa que pueda emitirse al respecto. La actualización deberá ser aprobada mediante Resolución Ministerial.

8. DIFUSIÓN

La difusión se realizará a todo el personal del MOPSV mediante la Dirección General de Asuntos Administrativos a través del Área de Normas.

9. CUMPLIMIENTO

Los diferentes aspectos contemplados en este documento son de obligatorio cumplimiento para todos los funcionarios, personal en comisión permanente, consultores y otros colaboradores del MOPSV

10. SANCIONES

En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, el MOPSV tomará las acciones disciplinarias y legales correspondientes, según normativa vigente.

III. CAPÍTULO III.- ALCANCE DEL PLAN METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACION

11. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Con la intensión de alinear la elaboración de un plan estándar, cuyas directrices son marcadas por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), el presente plan adopta para la gestión de riesgos, la guía incluida en el Anexo 1 de los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público, misma que toma como referencia la Metodología de Análisis y Gestión de Riesgos MAGERIT. En ese sentido y bajo los lineamientos dados se tomarán en cuenta los siguientes aspectos de la metodología:

a) Identificación, clasificación y valoración de Activos de Información.
b) Evaluación del Riesgo.
c) Tratamiento del Riesgo.
d) Controles implementados y por implementar.

Se destaca a la vez que, para delimitar y estandarizar el contexto tanto de las amenazas como de las vulnerabilidades de los activos de información, se tomaron como referencia el catálogo de amenazas de la Metodología MAGERIT y las vulnerabilidades expuestas en la norma ISO 27005.
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 Implementación 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.

11.1. 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 Implementación 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 valorará 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	UNID. RESP	RESPONSABLE	CUSTODIO	DISPONI-BILIDAD	INTE-GRIDAD	CONFIDEN-CIALIDAD	VALO-RACIÓN FINAL	FECHA INICIAL	FECHA FINAL
1	Infraestructura Tecnológica Física	Servidor de Procesamiento Almacenamiento Comunicación, Refrigeración, Energía	Equipamiento Informático, Redes de Comunicaciones	Centro de Procesamiento de Datos	UDTI	Responsable de Infraestructura Redes y Servicios	Responsable de Infraestructura Redes y Servicios	ALTO	ALTO	MEDIO	3.67	2024-09-19	2025-12-31
2	Infraestructura Tecnológica Virtual	En esta categoría están: servidores virtuales, discos virtuales	Soportes de Información	Centro de Procesamiento de Datos	UDTI	Responsable de infraestructura, servicios y redes	Responsable de infraestructura, servicios y redes	MUY ALTO	MUY ALTO	MUY ALTO	5.00	2024-09-19	2025-12-31
3	Base de datos	Datos e Información de todos los sistemas y servicios	Información	Centro de Procesamiento de Datos	UDTI	Responsable de Base de Datos	Responsable de Infraestructura redes y servicios	MUY ALTO	MUY ALTO	ALTO	4.67	2024-09-19	2025-12-31
4	Sistemas desarrollados	Sistemas desarrollado en la institución	Software - Aplicaciones Informáticas	Centro de Procesamiento de Datos	UDTI	Responsable de Desarrollo	Responsable de Infraestructura, redes y servicios	ALTO	ALTO	BAJO	3.33	2024-09-19	2025-12-31
5	Servicios	Servicios digitales brindados a los usuarios	Servicios	Centro de Procesamiento de Datos	UDTI	Responsable de Infraestructura, Redes y Servicios	Responsable de Infraestructura, Redes y Servicios	ALTO	MUY ALTO	ALTO	4.33	2024-09-19	2025-12-31
6	Redes de Comunicación a Internet	Redes de comunicación a internet	Redes de Comunicaciones	Centro de Procesamiento de Datos	UDTI	Responsable de Infraestructura, Redes y Servicios	Responsable de Infraestructura, Redes y Servicios	ALTO	MEDIO	BAJO	3.00	2024-09-19	2025-12-31
7	Red de Datos	Red de datos e interconexión	Redes de Comunicaciones	Centro de Procesamiento de Datos	UDTI	Responsable de infraestructura, Redes y Servicios	Responsable de infraestructura, Redes y Servicios	ALTO	MEDIO	MEDIO	3.33	2024-09-19	2025-12-31
8	Instalaciones físicas	Instalaciones físicas del CPD	Instalaciones	Oficinas del Ministerio de Obras Publicas Servicios y Vivienda	UDTI	Responsable de Infraestructura, Redes y Servicios	Responsable de Infraestructura, Redes y Servicios	ALTO	ALTO	ALTO	4.00	2024-09-19	2025-12-31

DGAA - U.A. VoBo Jean Mareño M.O.P.S.V.

DGAA - U.A. VoBo Jenny Panzi M.O.P.S.V.

12. 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.

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

12.1. Prioritarios

#	ACTIVO	AMENAZA	SITUACIÓN	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
1	Infraestructura Tecnológica Fisca	Fuego	Corto circuito	Carencia de sensores de humo y fuego	Probable	Crítico	ALTO
2	Infraestructura Tecnológica Fisca	Inundación	Inundación por fuga del agua en el sistema de aire acondicionado	carencia de sensores	Probable	Crítico	ALTO
3	Infraestructura Tecnológica Fisca	Desastres naturales	Terremotos	Carencia de sitio alterno	Poco Probable	Crítico	MEDIO
4	Infraestructura Tecnológica Fisca	Corte de suministro eléctrico	Corte de suministro de energía eléctrica	Falla en algún componente de la red	Muy Probable	Crítico	CRÍTICO
5	Infraestructura Tecnológica Fisca	Condiciones inadecuadas de	Altas temperaturas en el ambiente del CPD	Defectos en el equipamiento de	Muy Probable	Severo	ALTO
6	Infraestructura Tecnológica Virtual	Errores de mantenimiento	A la realización de mantenimientos preventivos o	Ausencia de procedimientos	Probable	Severo	ALTO
7	Infraestructura Tecnológica Virtual	Caída de sistema por agotamiento de recursos	Servidores virtuales no disponibles	Agotamiento de recursos	Probable	Severo	ALTO
8	Infraestructura Tecnológica Virtual	Errores de los usuarios	Errores en la manipulación por parte de los usuarios	Uso incorrecto de hardware o software	Poco Probable	Severo	MEDIO
9	Base de datos	Errores del Administrador	Daño por errores del administrador	Uso incorrecto de software y	Poco Probable	Severo	MEDIO
10	Base de datos	Difusión de software dañino	Daño en la base de datos por software dañino	Entrenamiento insuficiente en	Poco Probable	Crítico	MEDIO
11	Base de datos	Errores de Secuencia	Falla en el almacenamiento de Base de Datos	Software nuevo o inmaduro	Poco Probable	Severo	MEDIO
12	Base de datos	Destrucción de la información	Eliminación de la información	Ausencia de copias de respaldo	Poco Probable	Crítico	MEDIO
13	Base de datos	Errores de mantenimiento	Actualización de los programas	Configuración incorrecta de	Poco Probable	Severo	MEDIO
14	Base de datos	Perdida de Equipos	Equipos de almacenamiento con problemas	Ausencia de un eficiente control de cambios en la	Probable	Severo	ALTO
15	Base de datos	Indisponibilidad del Personal	personal fuera de la oficina o con algún impedimento de salud	Carencia de una persona que	Probable	Severo	ALTO
16	Sistemas desarrollados	Errores de usuarios	Mala operación con el sistema	ausencia de entrenamiento en el sistema	Probable	Moderado	MEDIO
17	Sistemas desarrollados	Errores del administrador	Fallo en el sistema o servicio	Ausencia de control de cambios eficaz	Poco Probable	Severo	MEDIO

18	Sistemas desarrollados	Errores de configuración	sistema con fallas de configuración	Configuración incorrecta de parámetros	Probable	Severo	ALTO
19	Sistemas desarrollados	Intercepción de la información	Envió de información	datos no encriptados	Probable	Moderado	MEDIO
20	Sistemas desarrollados	Repetición del mismo Incidentes en software	incidente repetido	carencia de habilidades para resolver el problema	Probable	Moderado	MEDIO
21	Servicios	Errores de configuración	Establecer configuraciones por defecto	Asignación errada de los derechos de acceso	Poco Probable	Severo	MEDIO
22	Servicios	Destrucción de la información	Al momento de manipular la información	ausencia de copias de respaldo	Probable	Crítico	ALTO
23	Servicios	Alteración accidental de información	Manipulación de información	Ausencia de control de cambios eficaz	Probable	Severo	ALTO
24	Servicios	Errores de mantenimiento o actualización de programas	Actualización o mantenimiento de servicios	Uso incorrecto de software y hardware	Probable	Severo	ALTO
25	Servicios	Caída de sistema por agotamiento de recursos	Concurrencia de uso del servicio	Configuración incorrecta de parámetros	Probable	Moderado	MEDIO
26	Redes de Comunicación a Internet	Fallos de servicios de comunicaciones	Corte del servicio de internet	carencia de proveedor alterno	Probable	Severo	ALTO
27	Red de Datos	Perdida de paquetes por campo electromagnético	En cualquier momento	Ausencia de medios ópticos	Probable	Severo	ALTO
28	Instalaciones físicas	Inundación	Fugas de agua en otros pisos	Ubicación en un área susceptible de inundación	Probable	Crítico	ALTO
29	Instalaciones físicas	Fuego	Incendio	Propagación de fuego de otras áreas	Probable	Crítico	ALTO

D.G.A.A. - U.A. VoBo Juan Moreno M.O.P.S.V.

D.G.A.A. - U.A. VoBo M.O.P.S.V.

D.G.A.A. - U.A. VoBo Juan Pelizi M.O.P.S.V.

12.2. No prioritarios

#	ACTIVO	AMENAZA	SITUACIÓN	VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
30	Base de datos	Alteración de información	Información alterada en la base de datos	Ausencia de terminación de la sesión cuando se abandona la estación de trabajo	Poco Probable	Moderado	**BAJO**
31	Sistemas desarrollados	Vulnerabilidad de los programas	modificación de información dentro el sistema	Configuración incorrecta de parámetros	Poco Probable	Moderado	**BAJO**
32	**Sistemas desarrollados**	**Vulnerabilidades de los programas**	**acciones realizadas dentro el programa por usuarios sin estándar**	**Habilitación de servicios innecesarios**	**Poco Probable**	**Moderado**	**BAJO**

12.3. Matriz de Valoración del Riesgo

CIERTA/INMINENTE	BAJO	MEDIO	ALTO	CRÍTICO	CRÍTICO
Muy Probable	BAJO	MEDIO	ALTO	ALTO 5	**CRÍTICO** **4**
Probable	IRRELEVANTE	BAJO	MEDIO 16, 19, 20, 25	ALTO 6, 7, 14, 15, 18, 23, 24, 26, 27	**ALTO** **1, 2, 22, 28, 29**
Poco Probable	IRRELEVANTE	BAJO	BAJO 30, 31, 32	MEDIO 8, 9, 11, 13, 17, 21	**MEDIO** **3, 10, 12**
Improbable	IRRELEVANTE	IRRELEVANTE	IRRELEVANTE	BAJO	**BAJO**
	Irrelevante	**Menor**	**Moderado**	**Severo**	**Crítico**

13. TRATAMIENTO DE RIESGO

Se tomaron 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
1	Infraestructura Tecnológica Fisca	Fuego	Corto circuito	Carencia de sensores de humo y fuego	Probable	Crítico	ALTO
2	Infraestructura Tecnológica Fisca	Inundación	Inundación por fuga del agua en el sistema de aire acondicionado	carencia de sensores	Probable	Crítico	ALTO
3	Infraestructura Tecnológica Fisca	Desastres naturales	Terremotos	Carencia de sitio alterno	Poco Probable	Crítico	MEDIO
4	Infraestructura Tecnológica Fisca	Corte de suministro eléctrico	Corte de suministro de energía eléctrica	Falla en algún componente de la red eléctrica comercial	Muy Probable	Crítico	CRÍTICO
5	Infraestructura Tecnológica Fisca	Condiciones inadecuadas de temperatura o humedad	Altas temperaturas en el ambiente del CPD	Defectos en el equipamiento de refrigeración	Muy Probable	Severo	ALTO
6	Infraestructura Tecnológica Virtual	Errores de mantenimiento	A la realización de mantenimientos preventivos o correctivos	Ausencia de procedimientos	Probable	Severo	ALTO
7	Infraestructura Tecnológica Virtual	Caída de sistema por agotamiento de recursos	Servidores virtuales no disponibles	Agotamiento de recursos	Probable	Severo	ALTO
8	Infraestructura Tecnológica Virtual	Errores de los usuarios	Errores en la manipulación por parte de los usuarios	Uso incorrecto de hardware o software	Poco Probable	Severo	MEDIO
9	Base de datos	Errores del Administrador	Daño por errores del administrador	Uso incorrecto de software y hardware	Poco Probable	Severo	MEDIO
10	Base de datos	Difusión de software dañino	Daño en la base de datos por software dañino	Entrenamiento insuficiente en seguridad	Poco Probable	Crítico	MEDIO
11	Base de datos	Errores de Secuencia	Falla en el almacenamiento de Base de Datos	Software nuevo o inmaduro	Poco Probable	Severo	MEDIO
12	Base de datos	Destrucción de la información	Eliminación de la información	Ausencia de copias de respaldo	Poco Probable	Crítico	MEDIO
13	Base de datos	Errores de mantenimiento	Actualización de los programas	Configuración incorrecta de parámetros	Poco Probable	Severo	MEDIO
14	Base de datos	Perdida de Equipos	Equipos de almacenamiento con problemas	Ausencia de un eficiente control de cambios en la configuración	Probable	Severo	ALTO

15	Base de datos	Indisponibilidad del Personal	personal fuera de la oficina o con algún impedimento de salud	Carencia de una persona que administre la base de datos	Probable	Severo	**ALTO**
16	Sistemas desarrollados	Errores de usuarios	Mala operación con el sistema	ausencia de entrenamiento en el sistema	Probable	Moderado	**MEDIO**
17	Sistemas desarrollados	Errores del administrador	Fallo en el sistema o servicio	Ausencia de control de cambios eficaz	Poco Probable	Severo	**MEDIO**
18	Sistemas desarrollados	Errores de configuración	sistema con fallas de configuración	Configuración incorrecta de parámetros	Probable	Severo	**ALTO**
19	Servicios	Errores de configuración	Establecer configuraciones por defecto	Asignación errada de los derechos de acceso	Poco Probable	Severo	**MEDIO**
20	Servicios	Destrucción de la información	Al momento de manipular la información	ausencia de copias de respaldo	Probable	Crítico	**ALTO**
21	Servicios	Alteración accidental de información	Manipulación de información	Ausencia de control de cambios eficaz	Probable	Severo	**ALTO**
22	Servicios	Errores de mantenimiento o actualización de programas	Actualización o mantenimiento de servicios	Uso incorrecto de software y hardware	Probable	Severo	**ALTO**
23	Servicios	Caída de sistema por agotamiento de recursos	Concurrencia de uso del servicio	Configuración incorrecta de parámetros	Probable	Moderado	**ALTO** **ALTO**
24	Redes de Comunicación a Internet	Fallos de servicios de comunicaciones	Corte del servicio de internet	carencia de proveedor alterno	Probable	Severo	**ALTO**
25	Red de Datos	Perdida de paquetes por campo electromagnétic	En cualquier momento	Ausencia de medios ópticos	Probable	Severo	**ALTO**
26	Instalaciones físicas	Inundación	Fugas de agua en otros pisos	Ubicación en un área susceptible de inundación	Probable	Crítico	**MEDIO**
27	Instalaciones físicas	Fuego	Incendio	propagación de fuego de otras áreas	Probable	Crítico	**MEDIO**
28	Sistemas desarrollados	Intercepción de la información	Envió de información	datos no encriptados	Probable	Moderado	**ALTO**
29	**Sistemas desarrollados**	**Repetición del mismo Incidentes en software**	**incidente repetido**	**carencia de habilidades para resolver el problema**	**Probable**	**Moderado**	**ALTO**

14. CONTROLES IMPLEMENTADOS Y POR IMPLEMENTAR

14.1. Listado de Controles Implementados y por Implementar

NRO.	CONTROL	SI/NO
1	5.3.1.iii. Implementar medidas de seguridad ambiental para minimizar riesgos de incendio, inundación, polvo, humedad, vibraciones, interferencia de suministro de energía, interferencia de las comunicaciones y radiación electromagnética.	si
2	5.3.1.iii. Implementar medidas de seguridad ambiental para minimizar riesgos de incendio, inundación, polvo, humedad, vibraciones, interferencia de suministro de energía, interferencia de las comunicaciones y radiación electromagnética.	si
3	10.1.1. ii. Implementar procesos y/o procedimientos de recuperación y restauración de operaciones críticas para cada evento identificado.	si
4	5.3.1. xv. De acuerdo a requerimientos de disponibilidad, se deberá implementar suministro alterno de energía eléctrica y/o banco de baterías.	si
5	5.3.1. ix. Se debe controlar la temperatura de operación del CPD.	si
6	5.3.1.i. Establecer procesos/procedimientos formales para la administración del CPD, en cuanto a accesos, mantenimiento de equipos, supervisión de trabajos externos y otros no limitativos a la	si
7	6.1.3.iii. Se deberá sacar de servicio a las aplicaciones, sistemas, bases de datos o entornos en desuso y/o obsoletos.	si
8	3.2.2.i. Capacitar y concientizar sobre las responsabilidades del uso de credenciales de acceso.	si
9	8.1.6.iii. Para la gestión de copias de respaldo, se deberán elaborar procesos / procedimientos que establezcan responsables, periodicidad y otros que se considere necesario.	si
10	8.1.6.i. Aplicar recomendaciones de configuración en seguridad provistas por el desarrollador del gestor de base de datos.	si
11	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
12	8.1.6.iii. Para la gestión de copias de respaldo, se deberán elaborar procesos / procedimientos que establezcan responsables, periodicidad y otros que se considere necesario.	si
13	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
14	6.1.1. iv. Se deberá documentar la instalación, configuración, recuperación, reinicio y mantenimiento de Infraestructura Tecnológica.	si
15	1.1.1. ii. Definir las restricciones y alcances del uso de la información, así como roles y responsabilidades.	si
16	1.2.1.i. Realizar eventos de concientización sobre la seguridad de la información, donde además se muestren roles y responsabilidades de los funcionarios para procedimientos de seguridad.	si
17	8.1.3. iv. Establecer procedimientos para el control de cambios, uso de repositorios seguros, documentar cambios funcionales y de seguridad a producción.	si
18	8.1.1. iv. Realizar procesos de gestión de actualizaciones de sistemas en caso de ser necesario. Todos los cambios deben ser probados, validados, evaluados, documentados y comunicados previamente.	si
19	8.1.1. iv. Realizar procesos de gestión de actualizaciones de sistemas en caso de ser necesario. Todos los cambios deben ser probados, validados, evaluados, documentados y comunicados previamente.	si
20	6.2.1.iii. Se deberán respaldar y restaurar la información y configuración de redes, bases de datos, servicios, servidores, servidores virtuales, entre otros.	si
21	8.1.3. iv. Establecer procedimientos para el control de cambios, uso de repositorios seguros, documentar cambios funcionales y de seguridad a producción.	si
22	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
22	11.1.1. iv. Implementar acciones correctivas y preventivas para lograr un proceso continuo, iterativo y de mejora continua del PISI.	si
23	6.1.2.iii. Los cambios de configuración deberán considerar el impacto asociado y realizarse en un ambiente controlado.	si

23	2.1.1. iv. Revisar y actualizar el inventario de activos de información mínimamente una vez al año y/o cuando se requiera.	si
24	7.1.1.iii. Considerar la implementación de dispositivos de red redundantes para puntos de fallo único donde la disponibilidad sea un factor crítico.	si
25	5.3.1. xiii. Se deberá organizar el cableado al interior del CPD, en lo posible cumplir con un cableado estructurado.	si
26	5.3.1.iii. Implementar medidas de seguridad ambiental para minimizar riesgos de incendio, inundación, polvo, humedad, vibraciones, interferencia de suministro de energía, interferencia de las comunicaciones y radiación electromagnética.	si
27	5.1.1.x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente.	si
28	4.1.1.iii. Utilizar cifrado para proteger la información en medios de almacenamiento, transferencia de archivos, información transmitida por redes de comunicación y otros que se considere necesario.	si
29	**9.1.1. iv. Los incidentes que no puedan ser solucionados deberán ser escalados al Centro de Gestión de Incidentes Informáticos por el RSI.**	**si**

14.1.1. Directriz

1.1.1. ii. Definir las restricciones y alcances del uso de la información, así como roles y responsabilidades.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Base de datos	ALTO	Indisponibilidad del Personal	Personal fuera de la oficina o con algún impedimento de salud	Carencia de una persona que administre la base de datos

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Establecer roles y responsabilidades	SI	NO	Incluir roles y responsabilidades para que al menos una persona tenga conocimiento de los accesos a las bases de datos.		

14.1.2. Directriz

1.2.1.i. Realizar eventos de concientización sobre la seguridad de la información, donde además se muestren roles y responsabilidades de los funcionarios para procedimientos de seguridad.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Sistemas desarrollados	MEDIO	Errores de usuarios	Personal fuera de la oficina o con algún impedimento de salud	Carencia de una persona que administre la base de datos

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Manuales de Operación	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.3. Directriz

2.1.1. iv. Revisar y actualizar el inventario de activos de información mínimamente una vez al año y/o cuando se requiera.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Servicios	MEDIO	Caída de sistema por agotamiento de recursos	Concurrencia de uso del servicio	Configuración incorrecta de parámetros

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Manuales de Operación	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.4. Directriz

3.2.2.i. Capacitar y concientizar sobre las responsabilidades del uso de credenciales de acceso.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Infraestructura Tecnológica Virtual	MEDIO	Errores de los usuarios	Errores en la manipulación por parte de los usuarios	Uso incorrecto de hardware o software

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Manuales de Operación	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.5. Directriz

4.1.1.iii. Utilizar cifrado para proteger la información en medios de almacenamiento, transferencia de archivos, información transmitida por redes de comunicación y otros que se considere necesario.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Sistemas desarrollados	MEDIO	Intercepción de la información	Envió de información	datos no encriptados

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Certificados	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.6. Directriz

5.1.1.x. Se deberá contar con equipamiento para mitigar posibles incendios, los cuales deben ser normados, revisados y probados periódicamente.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Instalaciones físicas	ALTO	Fuego	Incendio	propagación de fuego de otras áreas

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Infraestructura Tecnológica Virtual	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.7. Directriz

5.3.1.i. Establecer procesos/procedimientos formales para la administración del CPD, en cuanto a accesos, mantenimiento de equipos, supervisión de trabajos externos y otros no limitativos a la presente directriz.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Infraestructura Tecnológica Virtual	ALTO	Errores de mantenimiento	A la realización de mantenimientos preventivos o correctivos	Ausencia de procedimientos

D.G.A.A. - U.A. VoBo Ing. Marcelo M.O.P.S.V.

D.G.A.A. - U.A. VoBo Ing. Marcelo M.O.P.S.V.

D.G.A.A. - U.A. VoBo Jaime Patiri M.O.P.S.V.

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Manual de procedimientos	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.8. Directriz

5.3.1.iii. Implementar medidas de seguridad ambiental para minimizar riesgos de incendio, inundación, polvo, humedad, vibraciones, interferencia de suministro de energía, interferencia de las comunicaciones y radiación electromagnética.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Infraestructura Tecnológica Fisca	ALTO	Inundación	Inundación por fuga del agua en el sistema de aire acondicionado	carencia de sensores

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Sensores	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.9. Directriz

5.3.1.iii. Implementar medidas de seguridad ambiental para minimizar riesgos de incendio, inundación, polvo, humedad, vibraciones, interferencia de suministro de energía, interferencia de las comunicaciones y radiación electromagnética.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Infraestructura Tecnológica Fisca	ALTO	Fuego	Corto circuito	Carencia de sensores de humo y fuego

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Sensores	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.10. Directriz

5.3.1.iii. Implementar medidas de seguridad ambiental para minimizar riesgos de incendio, inundación, polvo, humedad, vibraciones, interferencia de suministro de energía, interferencia de las comunicaciones y radiación electromagnética.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Instalaciones físicas	ALTO	Inundación	Fugas de agua en otros pisos	Ubicación en un área susceptible de inundación

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Sensores	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.11. Directriz

5.3.1. ix. Se debe controlar la temperatura de operación del CPD.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Infraestructura Tecnológica Fisca	ALTO	Condiciones inadecuadas de temperatura o humedad	Altas temperaturas en el ambiente del CPD	Defectos en el equipamiento de refrigeración

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Sensores	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.12. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Red de Datos	ALTO	Perdida de paquetes por campo electromagnético	En cualquier momento	Ausencia de medios ópticos

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Cableado estructurado	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.13. 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	RIESGO	VULNERABILIDAD
Infraestructura Tecnológica Fisca	CRÍTICO	Corte de suministro eléctrico	Corte de suministro de energía eléctrica	Falla en algún componente de la red eléctrica comercial

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Suministro alterno de energía eléctrica	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

D.G.A.A. - U.A. VoBo Iván Mariaño M.O.P.S.V.

D.G.A.A. - U.A. VoBo M.O.P.S.V.

D.G.A.A. - U.A. VoBo Patzi M.O.P.S.V.

14.1.14. Directriz

6.1.1. iv. Se deberá documentar la instalación, configuración, recuperación, reinicio y mantenimiento de Infraestructura Tecnológica.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Base de datos	ALTO	Perdida de Equipos	Equipos de almacenamiento con problemas	Ausencia de un eficiente control de cambios en la configuración

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.15. Directriz

6.1.2.iii. Los cambios de configuración deberán considerar el impacto asociado y realizarse en un ambiente controlado.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Servicios	MEDIO	Caída de sistema por agotamiento de recursos	Concurrencia de uso del servicio	Configuración incorrecta de parámetros

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.16. Directriz

6.1.3.iii. Se deberá sacar de servicio a las aplicaciones, sistemas, bases de datos o entornos en desuso y/o obsoletos.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Infraestructura Tecnológica Virtual	ALTO	Caída de sistema por agotamiento de recursos	Servidores virtuales no disponibles	Agotamiento de recursos

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.17. Directriz

6.2.1.iii. Se deberán respaldar y restaurar la información y configuración de redes, bases de datos, servicios, servidores, servidores virtuales, entre otros.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Servicios	ALTO	Destrucción de la información	Al momento de manipular la información	ausencia de copias de respaldo

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Procedimiento de copias de respaldo	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.18. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Redes de Comunicación a Internet	ALTO	Fallos de servicios de comunicaciones	Corte del servicio de internet	carencia de proveedor alterno

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Proveedor Secundario	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.19. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Sistemas desarrollados	ALTO	Errores de configuración	sistema con fallas de configuración	Configuración incorrecta de parámetros

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.20. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Servicios	MEDIO	Errores de configuración	Establecer configuraciones por defecto	Asignación errada de los derechos de acceso

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.21. Directriz

8.1.3. iv. Establecer procedimientos para el control de cambios, uso de repositorios seguros, documentar cambios funcionales y de seguridad a producción.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Servicios	ALTO	Alteración accidental de información	Manipulación de información	Ausencia de control de cambios eficaz

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.22. Directriz

8.1.3. iv. Establecer procedimientos para el control de cambios, uso de repositorios seguros, documentar cambios funcionales y de seguridad a producción.

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Sistemas desarrollados	MEDIO	Errores del administrador	Fallo en el sistema o servicio	Ausencia de control de cambios eficaz

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.23. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Base de datos	MEDIO	Difusión de software dañino	Daño en la base de datos por software dañino	Entrenamiento insuficiente en seguridad

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.24. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Base de datos	MEDIO	Destrucción de la información	Eliminación de la información	Ausencia de copias de respaldo

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.25. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Base de datos	MEDIO	Errores del Administrador	Daño por errores del administrador	Uso incorrecto de software y hardware

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.26. 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	RIESGO	VULNERABILIDAD
Base de datos	MEDIO	Errores de Secuencia	Falla en el almacenamiento de Base de Datos	Software nuevo o inmaduro

D.G.A.A. - U.A. VoBo Iván Moreño M.O.P.S.V.

D.G.A.A. - U.A. VoBo Marco A. Ventura C. M.O.P.S.V.

D.G.A.A. - U.A. VoBo Jania Cauzi M.O.P.S.V.

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.27. 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	RIESGO	VULNERABILIDAD
Base de datos	MEDIO	Errores de mantenimiento	Actualización de los programas	Configuración incorrecta de parámetros

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.28. 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	RIESGO	VULNERABILIDAD
Servicios	ALTO	Errores de mantenimiento o actualización de programas	Actualización o mantenimiento de servicios	Uso incorrecto de software y hardware

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.29. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Sistemas desarrollados	MEDIO	Repetición del mismo Incidentes en software	incidente repetido	carencia de habilidades para resolver el problema

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Control de Cambios	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.30. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Infraestructura Tecnológica Fisca	MEDIO	Desastres naturales	Terremotos	Carencia de sitio alterno

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Continuidad del negocio	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.1.31. Directriz

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

ACTIVO	RIESGO	AMENAZA	RIESGO	VULNERABILIDAD
Servicios	ALTO	Errores de mantenimiento o actualización de programas	Actualización o mantenimiento de servicios	Uso incorrecto de software y hardware

Desarrollo

CONTROL DE SEGURIDAD DE LA INFORMACIÓN	INCLUSIÓN DEL CONTROL	CONTROL EXISTENTE	JUSTIFICACIÓN INCLUSIÓN	JUSTIFICACIÓN EXCLUSIÓN	DOCUMENTACIÓN
Continuidad del negocio	SI	NO	Control mínimo requerido. Resultados de la evaluación de riesgos		

14.2. Controles Mínimos de Seguridad de la Información

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

14.3. 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.

2024

#	CONTROL DE SEGURIDAD	INDICADOR Y MÉTRICA
1	5. Seguridad física y ambiental	Implementación de las medidas de seguridad física y ambiental al centro de procesamiento de datos
2	10. Plan de contingencias tecnológicas	Manual de plan de contingencias tecnológicas para el centro de procesamiento de datos
3	6. Seguridad de las operaciones	Lineamientos para la seguridad de las operaciones del centro de procesamiento de datos
4	3. Control de accesos	Implementar los controles de acceso biométricos para el centro de procesamiento de datos

5	8.Desarrollo, Mantenimiento y adquisición de sistemas	implementar políticas de desarrollo, mantenimiento y adquisición de sistemas para la institución hospedados en el centro de procesamiento de datos
6	1. Seguridad en recursos humanos	Implementar manuales de roles y funciones de los recursos humanos en el centro de procesamiento de datos
7	7. Seguridad de las comunicaciones	Implementar seguridad de las comunicaciones en base a configuraciones dentro el centro de procesamiento de datos

2025

#	CONTROL DE SEGURIDAD	INDICADOR Y MÉTRICA
1	10. Plan de contingencias tecnológicas	Manual de plan de contingencias tecnológicas para el centro de procesamiento de datos
2	6. Seguridad de las operaciones	Lineamientos para la seguridad de las operaciones del centro de procesamiento de datos
3	8.Desarrollo, Mantenimiento y adquisición de sistemas	implementar políticas de desarrollo, mantenimiento y adquisición de sistemas para la institución hospedados en el centro de procesamiento de datos
4	1. Seguridad en recursos humanos	Implementar manuales de roles y funciones de los recursos humanos en el centro de procesamiento de datos
5	7. Seguridad de las comunicaciones	Implementar seguridad de las comunicaciones en base a configuraciones dentro el centro de procesamiento de datos

IV. CAPÍTULO IV.- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Siguiendo los lineamientos expresados por la AGETIC, la Política de Seguridad de la Información (PSI) el Ministerio de Obras Públicas, Servicios y Vivienda, abarca los principios y posturas institucionales respecto a los dominios o ámbitos de seguridad desarrollados en el Anexo 1 de los Lineamientos para el PISI:

a) Seguridad en recursos humanos;
b) Gestión de activos de información;
c) Control de accesos;
d) Criptografía;
e) Seguridad física y ambiental;
f) Seguridad de las operaciones;
g) Seguridad de las comunicaciones;
h) Desarrollo, mantenimiento y adquisición de sistemas;

i) Continuidad de operaciones y gestión de incidentes de seguridad de la información;
j) Plan de contingencias tecnológicas;
k) Protección de información física documental
l) Cumplimiento.

De acuerdo al espectro de los controles identificados en las distintas áreas sustantivas del BCB, se redacta la Política de Seguridad de la Información (ver Anexo 1).

V. CAPITULO V.- CRONOGRAMA DE IMPLEMENTACIÓN

15. CONTROLES APLICADOS

La elaboración del Plan Institucional de seguridad de la información del Ministerio de Obras Públicas, Servicios y Vivienda, ha producido un inventario extenso de activos de información de las áreas sustantivas, una valoración a los riesgos de tales activos, y una identificación de controles por riesgo identificado.

Se priorizó la atención a los riesgos con valores críticos y altos, a través del análisis de riesgo. Asimismo, se diagramó el plan con actividades genéricas que tienen efecto en grupos de activos de información.

En ese sentido los controles aplicados de acuerdo al alcance del presente plan y a la priorización de los riesgos, se tiene la aplicación de los siguientes controles:

5. Seguridad física y ambiental
10. Plan de contingencias tecnológicas
6. Seguridad de las operaciones
3. Control de accesos
8.Desarrollo, Mantenimiento y adquisición de sistemas
1. Seguridad en recursos humanos
7. Seguridad de las comunicaciones

Luego de haber definido la estrategia, los objetivos y el alcance del plan de implementación del PISI, se determina el conjunto de actividades más importantes a ser realizadas o implementadas, los cuales considera la alineación de los objetivos de seguridad de información establecidos con el proceso de implementación seleccionado y a los controles de seguridad de información establecidos en los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad la Información de las entidades del sector público.

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.

16. ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN

Las actividades del plan fueron clasificadas como parte de uno de los siguientes grupos de estrategias de seguridad de la información:

1. Protección ante transacciones fraudulentas
2. Continuidad de operaciones y TI
3. Protección ante robo, pérdida o fuga de información
4. Oportunidad e integridad en las operaciones
5. Resguardo de material monetario, monedad conmemorativas y valores
6. Gobierno de Seguridad de la Información
7. Seguridad física y del Entorno

17. CRONOGRAMA DE IMPLEMENTACIÓN

Se realiza una revisión de los controles implementados y por implementar y se tiene el siguiente cronograma de implementación

#	CONTROL DE SEGURIDAD	ACTIVIDAD	ROLES Y RESPONSABILIDADES	2024 ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
1	5. Seguridad física y ambiental														
		Instalación del equipamiento necesario para brindar seguridad física y ambiental al centro de procesamiento de datos	Responsable de infraestructura, redes y									INI	X	X	X
2	10. Plan de contingencias tecnológicas														
		Manual de plan de contingencias tecnológicas para el centro de procesamiento de datos	Responsable de infraestructura, redes y									INI	X	X	X
3	6. Seguridad de las operaciones														
		Lineamientos para la seguridad de las operaciones del centro de procesamiento de datos	Responsable de infraestructura, redes y									INI	X	X	X
4	3. Control de accesos														
		Implementar los controles de acceso biométricos para el centro de procesamiento de datos	Responsable de infraestructura, redes y									INI	X	X	X
5	8. Desarrollo, mantenimiento y adquisición de sistemas														
		Implementar políticas de desarrollo, mantenimiento y adquisición de sistemas para la institución hospedados en el centro de procesamiento de datos	Responsable de desarrollo									INI:	X	X	X
6	1. Seguridad en recursos humanos														
		Implementar manuales de roles y funciones de los recursos humanos en el centro de procesamiento de datos	Jefe de Unidad de Recursos Humanos									INI	X	X	X
7	7. Seguridad de las comunicaciones														

D.G.A.A. - U.A. VoBo Janeth Paliz M.O.P.S.V.

		Implementar seguridad de las comunicaciones en base a configuraciones dentro el centro de procesamiento de datos	Responsable de infraestructura, redes y servidores								INI:	X	X	X	

2025

#	CONTROL DE SEGURIDAD	ACTIVIDAD	ROLES Y RESPONSABILIDADES	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
1	5. Seguridad física y ambiental														
		Instalación del equipamiento necesario para brindar seguridad física y ambiental al centro de procesamiento de datos	Responsable de infraestructura, redes y servidores	X	X	X	X	X	X	X	X	X	X	X	Fin
2	10. Plan de contingencias tecnológicas														
		Manual de plan de contingencias tecnológicas para el centro de procesamiento de datos	Responsable de infraestructura, redes y servidores	X	X	X	X	X	X	X	X	X	X	X	Fin
3	6. Seguridad de las operaciones														
		Lineamientos para la seguridad de las operaciones del centro de procesamiento de datos	Responsable de infraestructura, redes y servidores	X	X	X	X	X	X	X	X	X	X	X	Fin
4	8. Desarrollo, mantenimiento y adquisición de sistemas														
		implementar políticas de desarrollo, mantenimiento y adquisición de sistemas para la institución	Responsable de desarrollo	X	X	X	X	X	X	X	X	X	X	X	Fin
5	7. Seguridad de las comunicaciones														
		Implementar seguridad de las comunicaciones en base a configuraciones dentro el centro de procesamiento de datos	**Responsable de infraestructura, redes y servidores**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	Fin

D.G.A.A. - U.A. V°B° Iván Mareño M.O.P.S.V.

D.G.A.A. - U.A. V°B° M.O.P.S.V.

D.G.A.A. - U.A. V°B° Boris Panzi M.O.P.S.V.

ANEXO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

BICENTENARIO DE BOLIVIA

ESTADO PLURINACIONAL DE BOLIVIA

MINISTERIO DE OBRAS PÚBLICAS, SERVICIOS Y VIVIENDA

ESTADO PLURINACIONAL DE
BOLIVIA

MINISTERIO DE OBRAS PÚBLICAS, SERVICIOS Y VIVIENDA

DIRECCIÓN GENERAL DE ASUNTOS ADMINISTRATIVOS

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

D.G.A.A. - U.A. VoBo

D.G.A.A. - U.A. VoBo

D.G.A.A. - U.A. VoBo M.O.P.S.V.

26 NOV. 2024

La Paz – Bolivia

Contenido

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

El Ministerio de Obras Públicas, Servicios y Vivienda (MOPSV), destaca a la información institucional como un activo de alta importancia que posibilita el cumplimiento de sus objetivos. Esto genera la necesidad de implementar medidas de protección.

Para el MOPSV, la protección de la información busca la disminución del impacto generado sobre sus activos de información, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma.

Por esta razón, la Política de Seguridad de la Información (PSI), establece directrices que permiten definir estrategias para la protección de los activos de información ante amenazas que pudieran afectar su disponibilidad, integridad y confidencialidad, además del desarrollo de planes de continuidad de los sistemas de información, gestión de los riesgos y la respectiva implementación de los controles de seguridad de la información por parte del personal del MOPSV.

Para este fin, se cuenta con el compromiso de la Máxima Autoridad Ejecutiva de la Institución, Viceministros, Directores, Asesor, Gerentes, Jefes de Unidad y del personal de todas las Áreas y/o Unidades Organizacionales para la difusión, consolidación y cumplimiento de la presente Política.

2. TÉRMINOS Y DEFINICIONES

Los siguientes términos y definiciones son aplicables para el propósito del presente documento:

Activo. - En general, activo es todo aquello que tiene valor para la entidad o institución pública.

Activo de información. - Conocimientos o datos que tienen valor para la organización.

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.

Amenaza. - Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en la Institución. Se trata de un factor externo al activo de información, del que no se tiene control.

Apetito del riesgo. - Nivel máximo de riesgo que una entidad o institución está dispuesta a aceptar o soportar.

Comité de Seguridad de la Información (CSI). - Equipo de trabajo conformado para gestionar, promover e impulsar iniciativas en seguridad de la información.

Confidencialidad. - Propiedad que determina que la información no esté disponible ni sea revelada 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 de acceso y uso de información a entidades autorizadas cuando estas lo requieran.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Integridad. - Propiedad que salvaguarda la exactitud y completitud de la información.

Integridad de la información. - Propiedad que salvaguarda la exactitud y completitud de la información.

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.

Responsable del activo de información. - Servidor público de nivel jerárquico quien tiene la responsabilidad y las atribuciones de establecer los requisitos de seguridad y la clasificación de la información relacionada al activo de información enmarcado al proceso del cual es responsable.

Responsable de procesos. - Servidor público de nivel jerárquico que tiene la responsabilidad y atribución de establecer las actividades, roles y responsabilidades de los procesos.

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. - 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.

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.

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

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

Sistemas y Aplicaciones. - Diseñadas y administradas por la Unidad de Desarrollo Tecnológico e Información, son herramientas que permiten a los usuarios la interacción con la Institución y mejorar los procesos propios de cada Unidad Organizacional.

Vulnerabilidad. - Debilidad de un activo de información o control de seguridad que puede ser aprovechada por una amenaza. Es un factor interno del que se tiene control.

DEFINICIÓN DEL ALCANCE DEL PISI

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

El alcance del Plan Institucional de Seguridad de la Información en su primera versión tiene un alcance ligado específicamente al Centro de Procesamiento de Datos aprobado por el Comité de Seguridad de la Información, debido a que el Ministerio de Obras Publicas Servicios y Vivienda tiene sistemas y servicios digitales, traducidos en información digital. Todo el Plan Institucional de Seguridad de la Información será ejecutado hasta el año 2025, teniendo que realizarse actualizaciones en el tiempo que el Responsable de la Información o Comité de Seguridad de la Información vean necesario.

3. OBJETIVO GENERAL

Establecer las directrices que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información del MOPSV, teniendo en cuenta los objetivos, los procesos, las operaciones y los requisitos legales vigentes en la Entidad.

4. OBJETIVOS ESPECÍFICOS

- Puntualizar las políticas relacionadas con el análisis de riesgos e identificación de controles en los dominios relevantes.
- Fortalecer la concientización de la importancia de la seguridad de la información del MOPSV en el personal.
- Establecer políticas, reglamentos y procedimientos en materia de seguridad de la información
- Procurar la mejora continua de la continuidad de operaciones del MOPSV frente a amenazas de diferente índole.

5. ALCANCE

La Política de Seguridad de la Información es aplicable a todas las áreas y unidades organizacionales del MOPSV, a sus recursos, a los procesos internos o externos y a todo el personal de la entidad, cualquiera sea su situación laboral y el tipo de tareas que desempeñen.

6. ROLES Y RESPONSABILIDADES

a) **El Comité de Tecnología y Seguridad de la Información (CTSI)** es responsable proponer al Directorio del Ministerio de Obras Públicas, Servicios y Vivienda (MOPSV), la aprobación de la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.

b) **La Máxima Autoridad de Ejecutiva (MAE)** es responsable de cumplir y hacer cumplir la PSI y la normativa que se deprenda de ella al interior de su área.

c) **El (la) Responsable de Seguridad de la Información (RSI**) es el encargado de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información. Asimismo, tiene la función de proponer la Política de Seguridad de la Información.

d) **El (la) Jefe de la Unidad de Tecnología e Información (UDTI),** es responsable de cumplir funciones relativas a la seguridad informática de la entidad.

e) **El (la) jefe de Recursos Humanos** es responsable de promover la concientización y formación del recurso humano del MOPSV en seguridad de la información.

f) **El (la) Director General de Asuntos Jurídicos**, es responsable de asesorar en materia legal en lo que se refiere a la seguridad de la información.

g) **El (la) jefe de Auditoria Interna**, es responsable de llevar a cabo auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos y tecnología de información.

h) Todo **el personal del MOPSV**, es responsable de conocer y cumplir la PSI vigente.

a. 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.

b. 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.

c. DOCUMENTO DE CONFORMACIÓN Y FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Mediante Resolución Ministerial N° 286 de fecha 14 de septiembre de 2018 la Máxima Autoridad Ejecutiva designa al personal que conformará el Comité de Seguridad de la Información (CSI).

El CSI está 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.

7. DESARROLLO

La Política de Seguridad de la Información del MOPSV, se sustenta en el resguardo, protección y seguridad de la información que se genera, procesa y almacena. A este efecto, se ha definido un conjunto de directrices de alto nivel que permiten preservar la confidencialidad, disponibilidad e integridad de la información:

1. Establece que la información que genera, procesa y resguarda es de gran importancia para el ejercicio de sus atribuciones constitucionales y las establecidas en la ley 1670.
2. Protege los activos de información críticos, orientando sus esfuerzos a la preservación de la confidencialidad, integridad y disponibilidad de la información institucional, alineado al plan estratégico institucional (PEI).

En relación a los dominios de la seguridad el MOPSV establece las siguientes políticas:

DOMINIO DE SEGURIDAD / DESCRIPCIÓN	POSTURA INSTITUCIONAL
a) Seguridad en recursos humanos Es necesario establecer mecanismos de relación, en materia de seguridad de la información, entre el recurso humano y el **MOPSV** con el objetivo de preservar la información a la que tienen acceso durante y después de la vinculación laboral.	a) <u>Respecto a la protección de la información institucional ante amenazas que se originan del recurso humano.</u> 1. Concientizar, entrenar y capacitar al personal del MOPSV para implantar una cultura de seguridad de la información. 2. El personal deberá conocer, entender y asumir sus responsabilidades con respecto a la seguridad de la información. 3. Establecer responsabilidades y condiciones para manejo de la información a la que tienen acceso el personal del MOPSV y terceros; durante y después del vínculo laboral.

b) 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.

b) Respecto al uso y protección de activos de información.

4. Identificar y clasificar los activos de información en físico y digital, a fin determinar el tipo de activo y su grado de sensibilidad y criticidad.
5. Todo activo de información debe estar asignado a un área responsable de la entidad.
6. El uso del activo de información debe ser definido por el área responsable.
7. Priorizar la protección en base al grado de sensibilidad y criticidad del activo de información.
8. Priorizar la implementación de recursos tecnológicos, de infraestructura y recursos humanos para la adecuada protección de los activos de la información y gestión de medios de almacenamiento removibles.

c) Control de accesos

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

c) Respecto al control de accesos a recursos de red, información, sistemas y aplicaciones.

9. El acceso a los recursos de red, información, sistemas y aplicaciones, sistemas provistos por terceros, incluyendo el teletrabajo, debe contar con los niveles de autorización y mecanismos de protección acordes a la clasificación de activos de información.
10. El área responsable de los activos de información, debe asignar y revocar los accesos a recursos de red, información, sistemas y aplicaciones de acuerdo a las funciones.

d) 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 autenticación

d) Respecto a la protección de información transmitida a través de redes de comunicaciones

11. Los mecanismos de protección para la transmisión de información deben ser acordes a la sensibilidad y criticidad de la misma.

e) Seguridad física y ambiental

Asegurar áreas e instalaciones donde se genere, procese, transmita o almacene

e) Respecto a la protección de áreas e instalaciones donde se genere, procese, transmita o almacene

información considerada sensible y critica para el MOPSV, con el objetivo de prevenir accesos no autorizados que comprometan la seguridad de la información.

información considerada sensible y crítica

12. Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos del MOPSV.
13. Clasificar áreas e instalaciones en función a su sensibilidad y criticidad, implementar controles de acceso físico, monitoreo y vigilancia.
14. Disponer de elementos de seguridad para mitigar o transferir riesgos de origen natural, tecnológico o provocado por las personas.

f) Seguridad de las operaciones

Garantizar y asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta.

f) Respecto a la seguridad de las operaciones

15. Implementar controles para asegurar que las actividades operacionales en instalaciones de procesamiento de información se realicen de forma correcta y continua considerando la responsabilidad para la ejecución de las operaciones, protección contra pérdida de información y generación de respaldos de información.

g) Seguridad de las comunicaciones

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

g) Respecto a la seguridad de las comunicaciones

16. Implementar mecanismos de protección para la disponibilidad de la información en las redes de datos.
17. Gestionar de forma eficiente y segura el servicio de mensajería y correo electrónico para preservar la integridad y confidencialidad de la información transferida.

h) Desarrollo, mantenimiento y adquisición de sistemas

Establecer requisitos de seguridad para el desarrollo, mantenimiento y adquisición de sistemas que consideren pruebas de seguridad, pruebas de calidad y aceptación para desarrollos internos y externos.

h) Respecto a la seguridad en el ciclo de vida de los sistemas y/o software que se desarrolle y/o adquiera

18. Establecer e implantar requisitos de seguridad en el ciclo de vida de los sistemas, sean software vigentes o en proceso de implementación.

i) Continuidad de operaciones y gestión de incidentes de seguridad de la información

i) Respecto a la continuidad de las operaciones y procesos mediante

Establecer mecanismos para la gestión de incidentes en seguridad de la información dentro del MOPSV, para dar continuidad a las operaciones y mejorar los controles de seguridad implementados.	la gestión de incidentes en seguridad de la información. 19. Contar con recursos tecnológicos, humanos, infraestructura física y normativa para permitir la continuidad operativa de los procesos críticos. 20. Implementar, mantener y probar el Plan de Continuidad Operativa. 21. Gestionar los incidentes de seguridad de la información que afecten la continuidad operativa y gestionar las bitácoras de registro (LOGS). 22. La gestión de incidentes de seguridad de la información abarca la prevención, detección, respuesta y recuperación.
j) Plan de contingencias tecnológicas	j) Respecto al 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.	23. Contar con un Plan de Contingencias Tecnológicas formalizado, actualizado e implementado donde se asigne responsabilidades para su ejecución a los propietarios de los activos de información.
k) Protección de información física documental	k) Respecto a la protección de información física documental
Gestionar la seguridad de la información física documental de manera integral.	24. Evitar el robo, pérdida o modificación de documentos físicos mediante su resguardo seguro.
l) Cumplimiento	l) Respecto al 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	25. Revisar los controles evaluando periódicamente el cumplimiento de la normativa documental del Plan Institucional de Seguridad de la Información, verificando que los mismos se encuentran en operación. Asimismo, efectuar auditorías al Plan Institucional de Seguridad de la Información.

D.G.A.A. - U.A. VºBº Iván Mareño M.O.P.S.V.

D.G.A.A. - U.A. VºBº Janina Patizi M.O.P.S.V.

8. DIFUSIÓN

El Responsable de Seguridad de la Información (RSI), a través de la Gerencia General, es el encargado de difundir las políticas de seguridad de la información del MOPSV a todo el personal. Este documento deberá ser de libre acceso a través de la red intranet del MOPSV.

9. CUMPLIMIENTO

La presente Política de Seguridad de la Información es de cumplimiento obligatorio por todo el personal del MOPSV.

10. SANCIONES

El incumplimiento a las políticas de seguridad de la información del MOPSV , ya sea de forma intencional o por negligencia, será sancionado de acuerdo a normativa vigente.

11. HISTÓRICO DE CAMBIO

Elaboración	Revisión	Aprobación	Modificación
Janina Monica Pattzi Iporre 06/06/2024	Comité de Tecnologías y Seguridad de la información	MOPSV	Documento Inicial

Fotocopia Legalizada

RESOLUCIÓN MINISTERIAL N° 232

La Paz, 26 NOV. 2024

CONSIDERANDO:

El Parágrafo I del Artículo 103, de la Constitución Política del Estado, determina que el Estado garantizará el desarrollo de la ciencia y la investigación científica, técnica y tecnológica en beneficio del interés general.

El Parágrafo II del Articulo precitado señala: *"El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación."*

El Articulo 232 del texto Constitucional, determina: *"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 Artículo 3 de la Ley 1178, de 20 de julio de 1990, de Administración y Control Gubernamentales, establece que los sistemas de Administración y de Control se aplicarán en todas las entidades del Sector Público, sin excepción.

El inciso b) del Artículo 7 de la Ley precitada, determina que toda entidad pública organizará internamente, en función de sus objetivos y la naturaleza de sus actividades, los sistemas de administración y control interno de que trata esta ley.

El inciso g) del Artículo 7 de la Ley N° 2027, de 27 de octubre de 1999, del Estatuto del Funcionario Público, establece el derecho del servidor público a que se le proporcionen los recursos materiales necesarios para el cumplimiento de sus funciones.

El numeral 5 del Artículo 2 de la Ley N° 164, de 08 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación, señala como uno de los objetivos de la Ley, el de promoveré el uso de las tecnologías de información y comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos.

El numeral 38 del Parágrafo II del Artículo 6 de la Ley N° 64, define comoTecnologías de Información y Comunicación – TIC, al conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión y recepción de información, voz, datos, texto, video e imágenes. Se consideran como sus componentes el hardware, el software y los servicios.

El numeral 15 y 19 del Artículo 14 de la Ley N° 164, señalan entre las atribuciones de la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes el de elaborar, actualizar y modificar manuales, instructivos, circulares y procedimientos a ser aplicados en el sector y coordinar con los actores involucrados, el avance, desarrollo de las tecnologías de información y comunicación, brindando apoyo y asesoría técnica a nivel territorial y sectorial.

El Articulo 68, de la Ley N° 164, señala que el Ministerio de Obras Públicas, Servicios y Vivienda coordinará la articulación del Plan de Tecnologías de la Información y Comunicación con los planes de salud, educación, culturas, comunicación y demás planes sectoriales, que permitan la optimización de recursos, promoviendo el desarrollo de aplicaciones y la conectividad en todo el territorio del Estado.

El Parágrafo I del Artículo 72 de la Ley N° 164, 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 Artículo 76 de la Ley N° 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 inciso d) del Parágrafo II del Artículo 4 del Decreto Supremo N° 1793, de 13 de noviembre de 2013, Reglamento a la Ley N° 164, señala entre sus principios el de la Seguridad: *"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."*

El Articulo 8 del precitado Decreto Supremo, establece 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 inciso f) del Artículo 7 del Decreto Supremo N° 2514, de 09 de septiembre de 2015, determina como una de las funciones de la AGETIC la de establecer los lineamientos técnicos en seguridad de información para las entidades del sector público.

El inciso j) del Articulo precitado Articulo, señala como otra de las funciones de la AGETIC la de 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.

El Parágrafo I del Artículo 8 del Decreto Supremo N° 2514, crea el Centro de Gestión de Incidentes Informáticos- CGII como parte de la estructura técnica operativa de la AGETIC.

El inciso c) del Parágrafo II del Artículo 8 del Decreto Supremo N° 2514, establece los lineamientos para la elaboración de Planes de seguridad de Información de las entidades del sector público.

El Parágrafo III del Artículo 17 del Decreto Supremo N° 2514, señala que: ***"Las entidades del sector público deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII."***

El Plan Institucional de Implementación de Software Libre y Estándares Abiertos del Ministerio De Obras Públicas, Servicios y Vivienda, de 12 de junio de 2020, en el Punto 3.7 Sistemas y Servicios, en el inciso a) señala que el 25% de las aplicaciones esta en tecnologías privativas en su mayoría sistemas desarrolladas en NET. Estas aplicaciones son de vital importancia para el Ministerio puesto que simplifican tareas de procesos o tramites que se realizan dentro del Ministerio.

Mediante Nota Interna NI/MOPSV/DGAA/UDTI N° 0098/2024 I-2024-08481 de fecha 06 de noviembre de 2024, remitida por el Jefe de Unidad de Desarrollo Tecnológico e Información dependiente de la Dirección General de Asuntos Administrativos del Ministerio de Obras Públicas, Servicios y Vivienda, mediante el cual da conformidad al documento: "Plan Institucional de Seguridad de la Información (PISI) y Políticas de Seguridad de la Información (PSI).

Mediante Informe Técnico INF/MOPSV/DGAA/UA N° 0707/2024 I/2024-08481, de 12 de noviembre de 2024, emitido por la Encargada de Normas de la Dirección General de Asuntos Administrativos del Ministerio de Obras Públicas Servicios y vivienda, que concluye: *"A partir de lo expuesto, se considera que es viable la aprobación mediante Resolución Ministerial del "Plan Institucional de Seguridad de la Información (PISI) y Políticas de Seguridad de la Información (PSI)", para su aplicación en el Ministerio de Obras Públicas, Servicios y Vivienda, en el marco establecido en la normativa vigente..."*

El Informe Jurídico MOPSV – DGAJ N° 780/2024 I/2024-08481, de 22 de noviembre de 2024, emitido por la Dirección General de Asuntos Jurídicos del Ministerio de Obras Públicas, Servicios y Vivienda, concluye que de acuerdo a Informe Técnico INF/MOPSV/DGAA/UA N° 0707/2024, de 12 de noviembre de 2024, es legalmente viable aprobar mediante Resolución Ministerial el "Plan Institucional de Seguridad de la Información (PISI) conformado por cinco (5) capítulos y en anexo las Políticas de Seguridad de la Información (PSI)", para su aplicación en el Ministerio de Obras Públicas, Servicios y Vivienda, en el marco establecido en la normativa vigente.

El inciso w) del Parágrafo I del Artículo 14 del Decreto Supremo N° 4857, de 06 de enero de 2023, de Organización del Órgano Ejecutivo, establece como atribución de los Ministros de Estado, emitir resoluciones ministeriales en el marco de sus competencias.

POR TANTO:

El Ministro de Obras Públicas, Servicios y Vivienda, en ejercicio de sus atribuciones.

RESUELVE:

PRIMERO. - Aprobar el Plan Institucional de Seguridad de la Información (PISI) conformado por cinco (5) capítulos y en anexo las Políticas de Seguridad de la Información (PSI), que forman parte indivisible de la presente Resolución Ministerial, en el marco del Decreto Supremo N° 2514, de 09 de septiembre de 2015.

SEGUNDO. - Encargar el cumplimiento de la presente Resolución Ministerial a la Dirección General de Asuntos Administrativos del Ministerio de Obras Públicas, Servicios y Vivienda.

Regístrese, comuníquese y archívese.

Ing. Edgar Montaño Rojas
MINISTRO
Min. Obras Públicas, Servicios y Vivienda
ESTADO PLURINACIONAL DE BOLIVIA

MINISTERIO OBRAS PÚBLICAS, SERVICIOS Y VIVIEN.
DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
LEGALIZACIÓN: La presente fotocopia en fs. 3 (tres) es copia fiel del original de su referencia, que cursa en archivo de esta Dirección y al que en caso necesario me remito, por lo que se legaliza en cumplimiento de los arts. 1311 del Código Civil y 400 inc. 2) de su procedimiento. • Conste.
La Paz 26 de Noviembre de 2024
Abg. M. Luz Soruco Porcel
ABOGADO RESPONSABLE
UNIDAD DE ANALISIS JURIDICO
DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS
Min. Obras Públicas, Servicios y Vivienda

DESPACHO VºBº Abg. Edgar F. Landivar M. M.O.P.S.V.
VºBº Luis A. Cabrera M.O.P.S.V.
D.G.A.J. - U.G. VºBº Eduardo Gandarillas M.O.P.S.V.

EMR
LACP/ecp
C.c.: Arch.