POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) IMPLEMENTADO EN LA SECRETARÍA DE INVERSIONES PÚBLICO-PRIVADAS.

Tabla de contenido

1. Antecedentes

Que, el artículo 18, numerales 1 y 2 de la Constitución de la República del Ecuador (la **"Constitución"**) señala: *"Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información"*;

Que, el numeral 1 del artículo 154 de la Constitución determina: *"A las ministras y ministros de Estado, además de las atribuciones establecidas en la ley, les corresponde: 1. Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión"*;

Que, el artículo 226 de la Constitución establece: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución."*;

Que, el artículo 227 de la Constitución determina: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación"*;

Que, el artículo 5 letras a) y m) de la Ley Orgánica de Transparencia y Acceso a la Información Pública (la **"LOTAIP"**), señala: *"Principios. En el ejercicio del derecho de acceso a la información pública se aplicarán, además de los principios previstos en la Constitución de la República del Ecuador y en los instrumentos internacionales ratificados por el Estado, los siguientes: a) Accesibilidad e Integridad: La información entregada debe ser completa, comprensible, útil, fidedigna, veraz y estar disponible en formatos accesibles a través de un sistema de búsqueda simple y eficaz; m) Transparencia: Libre acceso a la información pública y de interés general."*;

Que, el artículo 7 de la LOTAIP establece: *"Derecho de acceso a la información pública. El derecho de acceso a la información pública comprende el derecho a buscar, acceder, solicitar, investigar, difundir, recibir, copiar, analizar, reprocesar, reutilizar y redistribuir información. Toda la información producida, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones establecidos en la presente Ley, la normativa vigente y en los instrumentos internacionales aprobados y ratificados por el Estado ecuatoriano. Cualquier persona, de forma individual o representando a una colectividad o cualquier grupo de personas, comunidad, pueblo o nacionalidad podrá*

solicitar el acceso a la información pública, teniendo los siguientes derechos: a) A ser informada si los documentos que contienen la información solicitada, o de los que se pueda derivar dicha información, obran o no en poder de la Autoridad Pública; b) Si dichos documentos obran en poder de la Autoridad Pública que recibió la solicitud, a que se le comunique dicha información en forma expedita; c) Si dichos documentos no se le entregan al solicitante, a apelar la no entrega de la información física y/o digital; d) A solicitar información sin tener que justificar las razones por las cuales se solicita; e) A no ser sujeto de cualquier discriminación que pueda basarse en la naturaleza de la solicitud; y, f) A obtener la información en forma gratuita o con un costo que no exceda el generado por la reproducción de los documentos. Ningún peticionario podrá ser sancionado por el ejercicio del derecho de acceso a la información pública.";

Que, el artículo 67 del Código Orgánico Administrativo señala: *"[...] El ejercicio de las competencias asignadas a los órganos o entidades administrativos incluye, no solo lo expresamente definido en la ley, sino todo aquello que sea necesario para el cumplimiento de sus funciones. [...]"*.

Que, mediante Decreto Ejecutivo No. 8 de 13 de agosto de 2009 publicado en el Registro Oficial No. 10 de 24 de agosto de 2009 el Presidente de la República creó el Ministerio de Telecomunicaciones y de la Sociedad de la Información como órgano rector del desarrollo de las Tecnologías de la Información y Comunicación;

Que, mediante Decreto Ejecutivo No. 107 de 2 de enero de 2024, el Presidente de la República designó al señor Mgs. Pablo José Cevallos Palomeque como Secretario de Inversiones Público Privado.

Que, mediante Acuerdo Ministerial MINTEL-MINTEL-2024-0003 de 08 de febrero de 2024 el Ministerio de Telecomunicaciones y de la Sociedad de la Información expide el Esquema Gubernamental de Seguridad de la Información EGSI V3.0 como mecanismo para implementar el sistema de gestión de seguridad de la información en el sector público.

Que, mediante Resolución No. SIPP-2024-0019 de 07 de octubre de 2024 el Secretario de la Secretaría de Inversiones Público – Privadas resolvió: *"Artículo 1: Delegar a el/la Coordinador/a General Administrativo Financiero para que, a nombre y representación del Secretario/a de Inversiones Público–Privadas, ejecute las siguientes atribuciones y responsabilidades: [...] b) Resolver la aprobación de normativa interna como instructivos, reglamentos, manuales y otros instrumentos exigidos por cualquier norma jurídica de cumplimiento obligatorio o que sean necesarios para la buena marcha de la Secretaría de Inversiones Público–Privadas"*.

Que, es necesario se emitan las Políticas de Seguridad de la Información en virtud del tipo de documentación que manejan los servidores y funcionarios de la Secretaría de Inversiones Público-Privadas.

Que, en ejercicio de las atribuciones constitucionales, legales, reglamentarias, y aquellas delegadas por la máxima autoridad.

2. Objetivo de la Política

Proporcionar las directrices para proteger y salvaguardar la información generada por las unidades administrativas de la Secretaría de Inversiones Público - Privadas y los recursos tecnológicos utilizados para su creación, procesamiento y administración, frente a amenazas internas o externas, intencionales o no, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad; implementando mecanismos que garanticen su autenticidad, que sea auditable, que no pueda ser duplicada para fines ajenos a los institucionales y que sus accesos no puedan ser repudiados.

3. Política de Seguridad de la Información

3.1. Descripción de la Política

Para las instituciones es importante contar con una Política de Seguridad de la Información, por lo que crear esta Política de Seguridad de la Información para la Secretaría de Inversiones Público-Privadas (SIPP) consiste en establecer un conjunto de directrices, normativas y procedimientos claros para proteger la información y los activos físicos y digitales de la entidad.

Esto resulta crucial para asegurar que los datos relacionados con los proyectos de inversión público-privada, así como los sistemas y redes que gestionan esa información, estén protegidos contra amenazas, vulnerabilidades y accesos no autorizados.

La máxima autoridad en conjunto con el Comité de Seguridad de la Información de la SIPP, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la SIPP.

Para la SIPP, la protección de la información busca la disminución del impacto generado sobre sus activos, 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 esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo expuesto, esta política aplica a la SIPP según como se defina en el alcance, sus funcionarios, terceros, proveedores y la ciudadanía en general.

3.2. Declaración de los objetivos de seguridad de la información

Objetivo 1: Garantizar la integridad, confidencialidad y disponibilidad de la información sensible, tanto a nivel interno como en colaboración con socios externos, como las empresas privadas involucradas en los proyectos; para ello resulta fundamental establecer roles y responsabilidades claras dentro de la SIPP para la gestión y protección de los datos, promoviendo un ambiente de cultura de seguridad dentro de la misma.

Objetivo 2: Asegurar que las prácticas de seguridad de la información estén alineadas con las leyes nacionales e internacionales, la Ley Orgánica de Protección de Datos Personales de Ecuador, y otros marcos regulatorios relevantes, como las normativas de seguridad y privacidad de datos del sector público y privado; esto fomentará la confianza entre los actores públicos y privados involucrados en los proyectos de inversión al demostrar un compromiso sólido con la protección de la información.

Objetivo 3: Minimizar los riesgos derivados de ataques cibernéticos, filtraciones de datos, o pérdidas de información debido a fallos técnicos o humanos. Esto permitirá mejorar la gestión de los recursos y asegurar un adecuado control de los recursos tecnológicos y humanos relacionados con la seguridad de la información, garantizando la continuidad de los proyectos y la eficiencia operativa.

Objetivo 4: Promover la formación continua del personal en temas de seguridad informática, ayudando a crear un entorno laboral consciente de los riesgos y buenas prácticas en el manejo de la información.

3.3. Roles y Responsabilidades

3.3.1. Máxima autoridad:

Dispone la difusión e implementación del Esquema Gubernamental de Seguridad de la Información, así como las Políticas de Seguridad de la información de la Secretaría de Inversiones Público – Privadas (SIPP)

3.3.2. Designación del Oficial de Seguridad de la Información:

La Máxima Autoridad será el encargado de designar al oficial de seguridad de la información (OSI) de la Secretaría de Inversiones Público – Privadas (SIPP).

3.3.3. Comité de Seguridad de la Información:

Cumple funciones enfocadas a mantener la política y normas institucionales particulares en materia de seguridad de la información, gestionar la aprobación y puesta en vigencia por parte de la máxima autoridad de la SIPP, así como el cumplimiento por parte de los servidores, funcionarios, trabajadores, asesores, practicantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP), para ello será el responsable de:

a) Monitorear cambios significativos de los riesgos que afectan a los recursos de información, frente a las amenazas más importantes.
b) Tomar conocimiento en la investigación y monitoreo de los incidentes relativos a la seguridad.
c) Aprobar las iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área.
d) Promover la difusión y apoyo a la seguridad de la información dentro de la SIPP.

e) Designar a los custodios o responsables de la información de las diferentes áreas de la SIPP, que deberá ser formalizada en un documento físico o electrónico.
f) Gestionar la promisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información.

3.3.4. Oficial de Seguridad de la Información:

Es el responsable de revisar el texto de la Política de Seguridad de la información, la estructuración, seguimiento y mejora del Sistema de Gestión de Seguridad de la SIPP, para lo cual deberá cumplir al menos lo siguiente:

a) Definir, coordinar y supervisar las estrategias de capacitación en coordinación con la Dirección de Administración del Talento Humano en materia de seguridad de la información, impulsando la implementación y cumplimiento de la presente política.
b) Controlar la aplicación de la política de protección de datos y privacidad de la información personal e implementar medidas técnicas y organizacionales apropiadas para gestionar de manera responsable la información personal de acuerdo con la legislación vigente y a lo establecido en el Esquema Gubernamental de Seguridad de la Información -EGSI, vigente.
c) Implementar de manera conjunta con las unidades administrativas de la Secretaría de Inversiones Público – Privadas (SIPP), mecanismos de carácter organizacional y tecnológico para autorización al acceso a la información, así como para el intercambio de datos personales o ciudadanos en custodia de la SIPP. Primará el principio de que los datos personales pertenecen a los ciudadanos y no a las instituciones en concordancia con la normativa legal vigente.
d) Implementar en coordinación con la Gestión Interna de Tecnologías de la Información y Comunicación medidas y mecanismos de seguridad física, lógica y procedimentales para la protección de la información digital de la SIPP.
e) Ejecutar revisiones independientes de la gestión de seguridad en las áreas que manejan información confidencial de la SIPP en intervalos planificados o cuando ocurran cambios, identifican las oportunidades de mejora y la necesidad de cambios con enfoque de seguridad, incluyendo la política y los objetivos de control.
f) Establecer mecanismos de comunicación y coordinación con los proveedores de servicios tecnológicos, así como mantenerse actualizado sobre las normativas y recomendaciones de seguridad del sector público, de modo que la política se adapte a los requerimientos legales y técnicos en evolución.
g) Dirigir el proceso de respuesta ante incidentes de seguridad, incluyendo la gestión, registro y escalamiento de estos.
h) Planificar y ejecutar auditorías internas y revisiones periódicas de seguridad en todos los sistemas.

El Oficial de Seguridad de la Información tendrá los siguientes roles y responsabilidades:

a) Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones y verificar su cumplimiento, de manera que no afecte la seguridad de la información.
b) Establecer criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas antes de su aprobación definitiva.
c) Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
d) Controlar los mecanismos de distribución y difusión de información dentro y fuera de la SIPP.
e) Definir y documentar controles para la detección y prevención de accesos no autorizados, protección contra software malicioso, garantiza la seguridad de los datos y servicios conectados a las redes de la SIPP.
f) Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas.
g) Verificar el cumplimiento de las políticas normas, procedimientos y controles de seguridad institucional establecidos y vinculados al EGSI.
h) Coordinarla gestión de eventos de seguridad con otras entidades gubernamentales.

Además, el Oficial de Seguridad de la Información en coordinación con la Dirección de Planificación y Gestión Estratégica a través de su Gestión Interna de Tecnologías de la Información y Comunicación deberá:

a) Controlar la existencia de documentación física y/o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.
b) Evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación.
c) Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
d) Monitorear las necesidades de capacidad de los sistemas en operación y proyectar futuras demandas de capacidad para soportar potenciales amenazas de seguridad a la información.
e) Procesar la obtención de copias de resguardo de información; así como la prueba periódica de su restauración.
f) Asegurar el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.
g) Desarrollar y verificar el cumplimiento de procedimientos para comunicar fallas en el procesamiento de la información o los sistemas de comunicaciones que permita tomar medidas correctivas.
h) Implementar y verificar los controles de seguridad definidos.
i) Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento e informes impresos, y verificar la eliminación o destrucción segura de los mismos.

j) Gestionar los incidentes de seguridad de la información de acuerdo con los procedimientos.
k) Realizar otras acciones vinculadas a su naturaleza en la gestión de seguridad de la información.

3.3.5. Director(a) de Planificación y Gestión Estratégica:

Se encarga de establecer, mantener y dar a conocer las políticas y procedimientos de los servicios de tecnología, incluida esta política de seguridad de la información y todos sus capítulos; el uso de los servicios tecnológicos en toda la SIPP, de acuerdo con las mejores prácticas y lineamientos institucionales y normativa vigente, para ello será el responsable de:

a) Mantener la custodia de la información que reposa en los diferentes sistemas, bases de datos y aplicativos internos de la SIPP.
b) Informar de los eventos que están en contra de la seguridad de la información e infraestructura tecnológica de la SIPP al Oficial de Seguridad de la Información, a las diferentes direcciones de la SIPP, así como a los entes de control e investigación que tiene injerencia sobre la misma.
c) La seguridad de la Gestión Interna de tecnologías de la Información y Comunicación y se encargará de definir y documentar controles para la detección y prevención de accesos no autorizados, protección contra software malicioso, garantiza la seguridad de los datos y servicios conectados a las redes de la SIPP.

3.3.6. Responsabilidades de las Unidades de la Dirección de Planificación y Gestión Estratégica.

Cumplirán con las siguientes responsabilidades:

a) Participar en el establecimiento, mantenimiento y divulgación de las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de la información y todos sus capítulos, el uso de los servicios tecnológicos en toda la SIPP de acuerdo con las mejores prácticas y lineamientos institucionales y normativa vigente a nivel del Gobierno
b) Mantener la custodia de la Información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la SIPP.
c) Informar los eventos que esté en contra de la seguridad: de la información y de la infraestructura tecnológica de la SIPP al Oficial de Seguridad de la Información, las diferentes Direcciones de la SIPP, así como a los entes de control o investigación que tienen injerencia sobre la misma.
d) Proporcionar las medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la SIPP.
e) Garantizar las condiciones tecnológicas óptimas para la implementación de las políticas de seguridad de información institucional.

f) Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de la Secretaría de Inversiones Público – Privadas (SIPP).
g) Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la SIPP.
h) Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la SIPP, esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.
i) Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas por parte de la Dirección de Planificación y Gestión Estratégica a través de la Gestión Interna de Tecnologías de la Información y Comunicación y las diferentes direcciones.
j) Implementar los mecanismos de control necesarios y pertinentes para verificar el cumplimiento de la presente política.

3.3.7. Responsabilidades de los Propietarios de la Información.

Los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la SIPP, que manejan, generan, procesan, reciben y almacenan en cualquier medio la información institucional, son responsables de:

a) Velar, valorar y clasificar la información que está bajo su administración y /o generación, siguiendo los lineamientos establecidos por la Constitución de la República del Ecuador, Ley Orgánica de Transparencia y Acceso a la Información Pública, el Esquema de Seguridad de la información y demás normativa relacionada con la materia.
b) Autorizar, restringir y delimitar a los demás usuarios de la SIPP el acceso a la información de acuerdo con sus roles y responsabilidades y a los diferentes servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP) que por sus actividades requieran consultar, crear o modificar parte o la totalidad de la información, así como la solicitud y aceptación de acuerdos de confidencialidad.
c) Determinar los tiempos de retención de la información juntamente con las áreas que se encarguen de su protección y almacenamiento de acuerdo con las normas vigentes y las políticas de la SIPP, así como de los entes externos y las normas o leyes vigentes.
d) Determinar y evaluar de forma periódica los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de esta.
e) Acoger e informar sobre las políticas de seguridad de la información a todos los servidores, funcionarios, trabajadores, asesores, consultores, proveedores,

practicantes/pasantes o cualquier persona que tenga relación con la SIPP, en las diferentes dependencias de esta, sobre su aplicación obligatoria.

3.3.8. Director(a) de Administración de Talento Humano.

El Director(a) de la Unidad de Administración de Talento Humano cumplirá la función de notificar a todo el personal que se vincula a la SIPP acerca de las obligaciones respecto del cumplimiento de las Políticas de Seguridad de la Información, de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de Seguridad de la Información y demás normativa interna, procedimientos y prácticas que se generan, para ello será el responsable de:

a) Socializar al personal, los cambios en las políticas de seguridad de la información que se presenten y de la suscripción del Acuerdo de Confidencialidad al personal que se vincula a la SIPP y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Oficial de Seguridad de la Información.

3.3.9. Personal General.

En el manejo y uso de la información, los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la SIPP y/o terceras personas que generan o acceden a la información de la SIPP, tienen las siguientes responsabilidades:

a) Manejar la información de la SIPP y rendir cuentas por el uso y protección de esta, mientras esté bajo su conocimiento y custodia, la que puede ser física o electrónica o almacenada en cualquier medio.
b) Proteger la información a la cual accedan o procesen, para evitar su pérdida, alteración destrucción o uso indebido.
c) No divulgar la información cuyo uso no esté autorizado, por las autoridades competentes.
d) Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de esta.
e) Informar a sus superiores, en el caso de terceros a cualquier persona que tenga relación con la SIPP, sobre la violación de estas políticas.
f) Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición, de la destrucción o alteración y de la divulgación no autorizada.
g) Reportar a la autoridad competente, los incidentes de seguridad, eventos sospechosos y mal uso de los recursos que identifique.
h) Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el cumplimiento de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenas a la SIPP, a la red Institucional ni el uso de dispositivos de acceso externo a internet o de difusión de señales de red que no hayan sido previamente autorizadas por el Oficial de Seguridad de la Información.

i) Utilizar el software autorizado adquirido legalmente por la SIPP. No está permitido la instalación ni uso de software diferente al institucional sin el consentimiento de sus superiores y visto bueno del Oficial de Seguridad de la Información.
j) Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección de Planificación y Gestión Estratégica a través de la Gestión Interna de Tecnologías de la Información y Comunicación en coordinación con el Oficial de Seguridad de la Información pueden solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web y redes sociales propiedad de la SIPP, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la SIPP. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por petición de las Máximas Autoridades, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.
k) Proteger y resguardar su información personal que no esté relacionada con sus funciones en la SIPP.
l) La SIPP no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al utilizar la infraestructura tecnológica facilitada por la SIPP.
m) Si un usuario cambia de equipo, ya sea por reemplazo de este o por traslado a otra unidad, el usuario deberá solicitar apoyo tecnológico a la unidad de Soporte a Usuarios mediante la herramienta dispuesta para el efecto.

3.3.10. Gestión de los Activos Fijos.

La Coordinación General Administrativa Financiera, a través de la Dirección Administrativa y sus gestiones internas, serán responsables de la gestión y manejo de activos que tienen valor para la SIPP, en colaboración con otras unidades y serán responsables de:

a) Inventariar activos primarios en formatos físicos y/o electrónicos conforme lo establece el Esquema de Seguridad de la Información y el Reglamento General Sustitutivo para la Administración, Utilización, Manejo y Control de los Bienes e Inventarios del Sector Público.
b) Inventariar los activos de Hardware, conforme lo establece el Esquema Gubernamental de la Información, donde consten equipos móviles, fijos, periféricos de salida, periféricos de entrada, dispositivos, sistemas ente otros vinculados a las acciones que ejecuta la SIPP y que permitan dar continuidad a las actividades logísticas y operativas.
c) Inventariar los activos de Software, Redes y demás aplicativos informáticos de la SIPP. Los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP), son responsables del manejo y uso de los activos de la SIPP que utiliza para sus actividades diarias.

El uso aceptable de los activos de la SIPP se enmarca en la utilización adecuada de los mismos y el cumplimiento de las normativas y políticas establecidas por la misma.

3.3.11. Gestión de Seguridad del Talento Humano:

Mediante sus gestiones internas son los responsables de ejecutar las siguientes acciones vinculadas al cumplimiento del Esquema Gubernamental de la información EGSI.

a) La Dirección de Administración del Talento Humano, verifica la información entregada por los candidatos previo a su contratación y entrega de manera formal las funciones y responsabilidades de los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que haya sido contratada:
b) Los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP), deberán firmar un acuerdo de confidencialidad y de no divulgación aprobado por el Comité de Seguridad de la Información, para acceder a la información confidencial.
c) La Dirección de Administración del Talento Humano en coordinación con el Oficial de Seguridad de la Información, deberá brindar una inducción a los nuevos funcionarios y servidores que se integran a la SIPP, donde expliquen las funciones, responsabilidades respecto a la seguridad de la información, acceso a la información, uso de contraseñas con sistemas de información confidencial.
d) Las Subsecretarías, Coordinaciones y Direcciones se encargan de explicar y definir las funciones y responsabilidades respecto a la seguridad de la información. Previa la terminación de un contrato laboral se debe realizar la transferencia de la documentación e información de la que fue responsable los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP) a la persona que designe el jefe inmediato; para garantizar la continuidad de las operaciones importantes dentro de la misma.

3.3.12. Gestión de Seguridad Física y del Entorno

La Dirección Administrativa es la responsable de disponer del personal adecuado para velar por el acceso y seguridad física a través del debido proceso de contratación o adquisición cuando su ubicación sea dentro o fuera de espacios públicos que no cuenten con las seguridades física necesarias de las áreas restringidas, así como de los equipos tecnológicos y personal; el acceso deberá ser controlado y restringido para el personal ajeno a estas áreas o usuarios externos, para lo cual se deben implementar normas, controles y/o registros de acceso.

Delegar un responsable del área de recepción, el cual controlará el acceso físico, deberá supervisar la permanencia de los visitantes en las áreas restringidas, debiendo registrar la hora, fecha de ingreso y salida, así como si ingresa con equipos o dispositivos tecnológicos, los cuales deben ser debidamente identificados y registrados.

Elaborar y remitir al Comité de Seguridad de la Información para aprobación, las directrices restrictivas en las áreas de procesamiento de información que evitarán poner en riesgo la conservación de los activos de información.

Coordinar con la Administración del Edificio la provisión del suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones de los servicios informáticos de la SIPP.

Coordinar con la Administración del Edificio obtener la documentación, diseños/planos y distribución de conexiones de: datos alámbricos/inalámbricas (locales y remotos), voz, eléctricas polarizadas, etc.

Proveer las barreras físicas o procedimientos que impidan el acceso a las áreas restringidas, pudiendo ingresar solamente el personal autorizado a ellas respetando el debido proceso de identificación.

3.3.13. Gestión de Comunicaciones y Operaciones:

Establece las normas que regulan esta Gestión, con el propósito de proteger la Información almacenada en los computadores dentro de la infraestructura tecnológica de la SIPP y minimizar los riesgos ante las amenazas que puedan surgir, para ello la Dirección de Planificación y Gestión Estratégica a través de su Gestión Interna de Tecnologías de la Información y Comunicación debe ejecutar lo siguiente:

a) Documentar los contactos de soporte y analizar los reportes de servicio, reportes de incidentes elaborados por terceros.
b) Monitorear los niveles de desempeño de los servicios; realizar proyecciones de necesidad institucional respecto de capacidad operativa y tecnológica para asegurar el desempeño de los servicios de la SIPP.
c) Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionadas con el servicio prestado.
d) Emitir normas reglamentarias de uso de software autorizados por la SIPP, que para el efecto se encargará a la unidad responsable de seguridad de información.
e) Debe instalar y actualizar de forma periódica el software antivirus y contra código malicioso, además debe, implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red como; firewalls, antivirus y demás mecanismos.
f) El Oficial de Seguridad de la Información, el responsable de la Gestión Interna de Tecnologías de la Información y Comunicación y el propietario de la información, deben determinar los procedimientos, etiquetado para el resguardo y contención de la información.
g) La Dirección de Planificación y Gestión Estratégica, a través de su Gestión Interna de Tecnologías de la Información y Comunicación es la responsable de documentar los incidentes y eventos incluyendo la hora, fecha, e información del evento, así como el registro y cuenta del administrador y operador que estuvo involucrado; además son corresponsables de la aplicación de políticas y normas para registrar los accesos, tipos

de accesos, protocolos de red, sistemas de protección como antivirus y sistemas de detección de intrusos y demás instrumentos que permita el manejo adecuado del negocio. Gestionar y normar las actividades vinculadas al numeral 6 del Esquema Gubernamental de Seguridad de la Información.

3.3.14. Gestión de Control de Acceso:

La Dirección de Planificación y Gestión Estratégica a través de la Gestión Interna de Tecnologías de la Información y Comunicación deberá regular el proceso de administración y control de accesos lógicos a los sistemas de información, con el fin de mitigar los riesgos de accesos y uso indebido de los mismos; para ello, se aplicarán las siguientes medidas:

a) Contribuir en la socialización de la Política de Control de Accesos para usuarios a los sistemas de información acorde al nivel y tipo.
b) Establecer normas y procesos formales para la asignación y cambio de contraseñas.
c) Determinar, diseñar y especificar el manejo de usuarios/as contraseñas y características especiales para la creación y uso de contraseñas como: uso de letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, que cumplan una complejidad media y alta para evitar contraseñas en blanco.
d) Controlar el cambio periódico de contraseñas e implementar medidas en el caso de que el usuario no está realizando ningún trabajo, el equipo se bloquee y lo desbloquee únicamente si el usuario ingresa nuevamente su clave.
e) Definir mecanismos para asegurar que la información transmitida por los canales de conexión remota, sean usando técnicas como encriptación de datos, redes virtuales privadas y otros que asegure la información.
f) Gestionar la Eliminación o deshabilitación de los puertos, y/o servicios que no requiera la SIPP.
g) Establecer un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros
de alarmas cuando se violan las políticas de seguridad del sistema.
h) Identificar y documentar los equipos que se encuentran en las redes, así como realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentra los activos críticos para la SIPP.

3.3.15. Gestión de Adquisición y Mantenimiento de Sistemas de Información:

El Comité de Seguridad de la Información es responsable de establecer normas de seguridad y controles durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan, por ello se realizará lo siguiente:

a) Implementar de manera conjunta entre la Dirección de Planificación y Gestión Estratégica a través de su Gestión Interna de Tecnologías de la Información y Comunicación, así como con el Oficial de Seguridad de la Información, la política de controles y gestión de claves, así como su generación.

b) Emitir y socializar la Política sobre el uso de controles criptográficos acorde a los requerimientos de seguridad de la información y el tipo de información, actividad que será realizada por el Oficial de Seguridad de la Información.
c) Establecer normas de controles de cifrado (criptográficos) que se adoptan, para la implementación eficaz en toda la SIPP; establece la solución a usar para cada proceso del negocio.
d) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas por alguna falla o falta de seguridad.

3.3.16. Consideraciones de la Seguridad de la información con actores externos (Ciudadanos o entidades gubernamentales o de control):

Previo a la entrega de información a ciudadanos o interesados por parte de las entidades gubernamentales o de control, las unidades responsables de proveer la información solicitada deberán consideran los siguientes criterios:

a) Autorización de la máxima autoridad o su delegado.
b) Tipo de información solicitada.
c) Protección de activos de información.
d) Protección de datos en base a la Constitución, Ley del Sistema Nacional de Registro de Datos Públicos, LOTAIP y demás Leyes nacionales aplicables a los planes, programas y proyectos de la SIPP, particularmente datos personales de ciudadanos y/o financieros.
e) Convenios para gestión o intercambio de información, incidentes de la seguridad de la información y violaciones de la seguridad.
f) Cumplimiento de Políticas de control de accesos.
g) Entendimiento adecuado en los acuerdos de confidencialidad de la información entre la SIPP y el solicitante con el objeto de cumplir los requisitos de la seguridad de la misma.

3.3.17. Gestión de Incidentes Informáticos:

Se establece los lineamientos generales para la gestión efectiva de incidentes de seguridad que afecten a la SIPP y al cumplimiento de su misión y objetivos, con la finalidad de prevenir y responder de forma idónea, para lo cual, la Dirección de Planificación y Gestión Estratégica mediante su Gestión Interna de Tecnologías de la Información y Comunicación debe realizar las siguientes acciones:

a) Implementar y ejecutar el procedimiento formal para el reporte de eventos de seguridad informáticos junto al procedimiento de escalada y respuesta al incidente que amenace la seguridad informática. Este procedimiento inicia mediante la mesa de servicios.
b) Mantener una bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, el monitoreo de los sistemas, alertas y las vulnerabilidades, se establece y ejecuta un procedimiento para la gestión de incidentes.

c) Identificar y clasificar los diferentes tipos de incidentes de seguridad de la información mediante la mesa de servicios y con la utilización de la matriz de asignación de responsabilidades-matriz RACI.
d) Identificar y analizar las posibles causas de un incidente producido.
e) Planificar e implementar acciones conectivas para evitar la recurrencia del incidente.
f) Establecer procesos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la SIPP.

Los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP), de turno que sea responsable del equipo o sistema afectado debe identificar, registrar el incidente en la bitácora incluyendo datos, fecha y hora, así como el tipo de incidente suscitado y el nivel de severidad de este.

En caso de que los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de turno no puedan solucionarlo, el escalamiento debe ser registrado en la bitácora de escalamiento de incidentes, se notificará al jefe inmediato.

3.3.18. Gestión de Incidentes de la Seguridad de la Información:

En caso de que los incidentes informáticos que produzcan afectación en la Seguridad de lo Información de esta SIPP, el Oficial de Seguridad de la Información es el contacto para el reporte de los eventos de seguridad de la información. Los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP) y usuarios contratados por los proveedores deben reportar todos los eventos de inseguridad de la información lo más pronto posible.

Los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP) y usuarios contratados por los proveedores de la SIPP, deben informar los asuntos de las debilidades en la seguridad al Comité de Seguridad de la Información o a su proveedor del servicio tan pronto como sea posible.

Cuando se detecte alguna vulnerabilidad o debilidad en un equipo o sistema se debe:

a) Informar y notificar a su jefe inmediato y este al Oficial de Seguridad de la Información la debilidad y vulnerabilidad encontrada.
b) El Oficial de Seguridad de la Información debe llevar el reporte de vulnerabilidades y debilidades de seguridad de la información, que contendrá la fecha, hora, apellidos, nombres de los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP) que detectó la debilidad, descripción

de la misma, detalle de posibles incidentes de seguridad que pudieran ocurrir como producto de la vulnerabilidad.

c) El Oficial de Seguridad de la información debe emitir un reporte del o los incidentes ocurridos a los jefes de las unidades donde se produjo el incidente.
d) El Oficial de Seguridad de la Información en coordinación con la Gestión Interna de Tecnologías de la Información y Comunicación realizarán una evaluación del impacto generado por el o los incidentes de seguridad de la información producidos donde se evidencie el tipo de incidente, el número de incidentes graves, el tiempo medio de resolución de incidentes, costo promedio de incidentes, frecuencia del incidente.

3.4. Alcance y usuarios

El presente instrumento, regirá a todos los servidores, funcionarios, trabajadores, asesores, practicantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP), inclusive para proveedores externos vinculados a la SIPP a través de contratos, convenios o acuerdos; y, con apego a la definición de roles y perfiles relacionados con el Esquema Gubernamental de Seguridad de la información (EGSI).

3.5. Comunicación de la Política

El Comité de Seguridad de la Información conjuntamente con la Dirección Administrativa del Talento Humano y la Dirección de Planificación y Gestión Estratégica, serán responsables de elaborar estrategias de socialización y capacitación a todos los servidores, funcionarios, trabajadores, asesores, consultores, proveedores, practicantes/pasantes o cualquier persona que tenga relación con la Secretaría de Inversiones Público – Privadas (SIPP) sobre el Esquema Gubernamental de la Información (EGSI) y de la Política de Seguridad de la información y sus Anexos, en un plazo de 60 días a partir de la vigencia de la presente Política.

3.6. Excepciones y sanciones

En caso de detectar incumplimiento de esta política, el Director (a) de la unidad administrativa pondrá en conocimiento del Oficial de Seguridad de la Información (OSI), la transgresión de la Política de Seguridad establecida en el presente instrumento y demás normativa relacionada, para ello el Oficial de Seguridad de la Información levantará un informe que será puesto en conocimiento de la Dirección de Administración del Talento Humano y a la máxima autoridad.

Cuando los responsables de las unidades administrativas omitan notificar al Oficial de Seguridad de la información (OSI) sobre las transgresiones de la Política de Seguridad de la información e instrumentos vinculantes, se pondrá en conocimiento de la máxima autoridad.

La divulgación o uso de la información que ocasionen el incumplimiento del presente instrumento podrá ser sancionado por el delito de difusión de información de circulación restringida o cualquier otro delito tipificado en el Código Orgánico Integral Penal, y leyes conexas; para lo cual, la Secretaría de Inversiones Público-Privadas (SIPP) se reserva el derecho de iniciar

las acciones administrativas, civiles o penales de las que se crea asistido, incluyendo la reclamación de daños y perjuicios sin límite alguno.

Cualquier uso malicioso, ilegal o fraudulento de la información estará sujeto al procesamiento penal de su responsable, sin perjuicio de las demás acciones legales a las que hubiere lugar, así como de la determinación del régimen disciplinario correspondiente. Los mencionados informes, servirán de insumo para lo determinado en líneas precedentes.

4. Glosario de términos

Término	Definición
Activo de información:	Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Institución y, en consecuencia, debe ser protegido.
Principios de No Repudio:	El no repudio es considerado uno de los principios fundamentales de seguridad de la información. Este principio es un servicio que garantiza que una persona no pueda negar haber realizado una acción en un sistema digital. También se le conoce como irrenunciabilidad; es decir, provee garantía al receptor de una comunicación en cuanto que el mensaje fue originado por el emisor y no por alguien que se hizo pasar por este. Además, previene que el remitente o emisor del mensaje afirme que él no envió el mensaje.
Activos de información:	Información de propiedad de la Secretaría de Inversiones Público-Privadas (SIPP), sus medios de almacenamiento y procesamiento, que son considerados críticos para el cumplimiento de los procesos y objetivos de la Institución.
Acción correctiva:	Medida implementada para eliminar la causa raíz de una no conformidad, con el fin de evitar su recurrencia en el futuro.
Acuerdo de confidencialidad:	Es un documento en el que, los servidores, funcionarios, trabajadores, asesores, practicantes y cualquier persona que tengan relación con la Secretaría de Inversiones Público-Privadas (SIPP) o los provistos por terceras partes, manifiestan su voluntad de mantener la confidencialidad de la información de la institución, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan.

Administración de riesgos:	Comprende el proceso de control y minimización, o la completa eliminación de los riesgos de seguridad que podrían afectar a la información de la Institución.
Análisis de riesgo de seguridad de la información:	Es un proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
Comité de Seguridad de la Información:	Grupo directivo conformado por representantes de diversas áreas de la institución, encargado de tomar decisiones estratégicas en materia de seguridad de la información y aprobar planes de acción derivados de la evaluación interna.
Custodio del activo de la información:	Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
Criterios de evaluación:	Conjunto de parámetros utilizados para determinar el nivel de cumplimiento de los controles de seguridad en una organización, basados en evidencias recopiladas durante la evaluación interna.
Dominio:	Es el conjunto de computadoras conectadas en una red informática que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.
EGSI	Esquema Gubernamental de Seguridad de la Información. Conjunto de normas, directrices y controles diseñados para garantizar la protección de la información en entidades gubernamentales, asegurando la confidencialidad, integridad y disponibilidad de los datos.
SGSI:	Sistema de Gestión de Seguridad de la Información. Marco estructurado de políticas, procedimientos y controles implementados en una organización para gestionar los riesgos de seguridad de la información y garantizar la protección de los activos de información.
Evaluación Interna:	Proceso sistemático de revisión y análisis del cumplimiento de los controles de seguridad de la información dentro de una

	institución, con el objetivo de identificar vulnerabilidades, no conformidades y oportunidades de mejora.
Evaluación de riesgos:	Comprende las acciones realizadas para identificar y analizar las amenazas y/o vulnerabilidades relativas a la información y a los medios de procesamiento de esta, así como la probabilidad de ocurrencia y el potencial impacto a las operaciones de la Institución.
Evidencia recopilada:	Información documentada que respalda los hallazgos identificados en la evaluación interna, pudiendo incluir registros, informes, configuraciones de sistemas, entrevistas y observaciones.
Hallazgo:	Cualquier deficiencia, vulnerabilidad o incumplimiento detectado durante la evaluación interna en relación con los controles de seguridad de la información establecidos en el EGSI.
Incidente de seguridad informática:	Es un intento de acceso, uso, divulgación, modificación o destrucción no autorizados de Información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o, cualquier otro acto que implique una violación a la Política de Seguridad de la Información de la SIPP.
Incidente de seguridad:	Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).
Información:	Se refiere a toda representación de conocimiento en forma de datos vinculados entre sí. Pudiendo ser textual, numérica, gráfica, cartográfica, narrativa o audiovisual, almacenada en cualquier medio, ya sea magnético, en papel, en medios electrónicos computadoras, audiovisual u otras.
Información sensible:	Es aquella a la cual la ley tiene prohibido divulgar, ya que perjudica la seguridad nacional, o la intimidad personal; por ejemplo, ciertos datos personales y bancarios, contraseñas de correos electrónicos. Estos son datos personales que solo pueden ser revelados con autorización del titular.

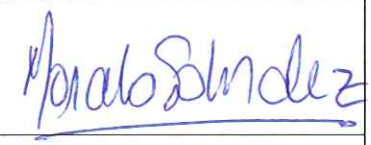
Indicadores de Seguridad de la Información:	Métricas utilizadas para evaluar el nivel de cumplimiento de los controles de seguridad en la organización y medir la efectividad de las medidas implementadas.
Informe de evaluación interna:	Documento oficial que contiene el análisis detallado de la evaluación realizada, incluyendo hallazgos, evidencias, nivel de cumplimiento y recomendaciones para la mejora del SGSI.
No conformidad:	Incumplimiento de un requisito de seguridad de la información establecido en el EGSI o en las normativas internas de la institución. Puede clasificarse como mayor (cuando existe un riesgo significativo para la seguridad) o menor (cuando el impacto es limitado o parcial).
(OSI) - Oficial de Seguridad de la Información:	Responsable de supervisar la implementación y cumplimiento de las políticas y controles de seguridad de la información dentro de una organización, garantizando la alineación con el EGSI y otras normativas aplicables.
Oportunidad de mejora:	Situaciones detectadas en la evaluación interna que, aunque no constituyen no conformidades, representan áreas donde la seguridad de la información puede fortalecerse para mejorar la eficiencia y la protección de los datos
Presentación de resultados:	Estrategia de comunicación utilizada para exponer los hallazgos de la evaluación interna ante la alta dirección y otras partes interesadas, con el propósito de facilitar la toma de decisiones y priorizar la implementación de mejoras en seguridad de la información.
Plan de acción:	Estrategia documentada que detalla las medidas correctivas y preventivas a implementar para remediar no conformidades detectadas, estableciendo responsables, plazos de ejecución e indicadores de seguimiento.
Priorización de hallazgos:	Clasificación de los hallazgos según su criticidad y riesgo potencial, con el fin de definir el orden en que deben ser abordados para mitigar impactos en la seguridad de la información.
Seguimiento y monitoreo:	Proceso continuo de revisión y control de la implementación de las acciones correctivas y preventivas establecidas en el plan de acción, para verificar su efectividad.
Valoración del cumplimiento:	Metodología utilizada para medir el nivel de implementación de los controles de seguridad de la información en una

	organización, con base en un rango de cumplimiento del 0% al 100%.

5. Documentos de referencia

- Ley Orgánica para la Transformación Digital y Audiovisual
- Ley Orgánica de Protección de Datos Personales
- Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)
- Normas Técnicas ISO/IEC 27000
- Alcance del Esquema Gubernamental de Seguridad de la Información
- Plan estratégico institucional
- Otros.

6. Firmas de responsabilidad

	Nombre/Cargo	Firma
Elaborado por:	Marcelo Sánchez **Oficial de Seguridad de la Información**	
Revisado y Aprobado por:	Freddy Romero **Presidente del Comité de Seguridad de la Información**	

Control de versiones del formato referencial

Versión:	1.0
Fecha de la versión:	01-03-2024
Creado por:	Dirección de Infraestructura, Interoperabilidad, Seguridad de la Información y Registro Civil
Aprobado por:	Subsecretaría de Gobierno Electrónico y Registro Civil
Nivel de confidencialidad:	Bajo

Historial de cambios del formato referencial

Versión	Fecha	Detalle del cambio

1.0	01/03/2024	Emisión inicial del documento