2025

Empresa Metropolitana EPMSA

Quito Alcaldía Metropolitana

Política de Seguridad de la Información de la EPMSA

GERENCIA GENERAL

Versión 1.0

EMPRESA PÚBLICA METROPOLITANA DE SERVICIOS AEROPORTUARIOS Y GESTIÓN DE ZONAS FRANCAS Y REGÍMENES ESPECIALES - EPMSA | www.aeropuertoquito.com

CONTROLES - FIRMAS DE RESPONSABILIDAD

Elaboración de la Política de Seguridad de la Información y Aprobación técnica

APROBACIÓN	FIRMA
Sebastián Nader **Gerente General**	Firmado electrónicamente por: SEBASTIAN ALFREDO NADER .
REVISIÓN	**FIRMA**
Sergio Yamni Tamayo Piedra **Gerente de Planificación y Proyectos**	Firmado electrónicamente por: SERGIO YAMNI TAMAYO PIEDRA
ELABORACIÓN	**FIRMA**
Mario Francisco Verdesoto Vallejo **Analista de Control de Calidad AVSEC** **Oficial de Seguridad de la Información**	Firmado electrónicamente por: MARIO FRANCISCO VERDESOTO VALLEJO

Asesoría metodológica

ELABORACIÓN	FIRMA
Cristian Alulema **Analista de Planificación 1**	Firmado electrónicamente por: CRISTIAN BAYARDO ALULEMA ROBALINO

Control e historial de cambios

Versión	Fecha	Descripción del cambio
1.0	19/02/2025	Creación de la Política de Seguridad de la Información de la EPMSA

Tabla de contenido

1. Antecedentes

La generalización de los servicios a través de las tecnologías de la información ha convertido a la información en un activo valioso para las instituciones públicas, y su pérdida o manipulación indebida puede afectar gravemente la confianza ciudadana, generar procesos legales y dañar la reputación institucional.

En este contexto, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) ha creado el Esquema Gubernamental de Seguridad de la Información (EGSI v3) que es un Sistema de Gestión que establece políticas, directrices y recomendaciones para garantizar la seguridad de la información en el sector público, promoviendo una mejora continua en su gestión.

"[…] El Ministerio de Telecomunicaciones y de la Sociedad de la Información mediante Acuerdo Nro. Minte-Mintel-2024-0003 de fecha 01 de marzo de 2024 expidió el Esquema Gubernamental de Seguridad de la Información – EGSI el cual es el mecanismo para implementar el sistema de gestión de seguridad de la información en el sector público, emitiendo los siguientes acuerdos:

Artículo 1.- Expedir el Esquema Gubernamental de Seguridad de la Información – EGSI que se encuentra como Anexo al presente Acuerdo Ministerial, el cual es el mecanismo para implementar el Sistema de Gestión de Seguridad de la Información en el Sector Público.

Artículo 2.- El EGSI es de implementación obligatoria en las entidades, organismos e instituciones del sector público, de conformidad con lo establecido en el artículo 225 de la Constitución de la República del Ecuador y los artículos 7 literal o), y 20 de la Ley Orgánica para la Transformación Digital y Audiovisual; y, además, es de implementación obligatoria para terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas, quienes podrán incorporar medidas adicionales de seguridad de la información.[…]"

La información es un recurso importante para la Empresa Pública Metropolitana de Servicios Aeroportuarios y Gestión de Zonas Francas y Regímenes Especiales (EPMSA), esencial para el progreso de su misión y el cumplimiento de sus objetivos estratégicos.

El avance en tecnologías de la información ha permitido optimizar las operaciones empresariales, pero su uso indebido puede exponer a la empresa a amenazas que comprometan la integridad de los datos. Ante estos riesgos, EPMSA implementará un Sistema de Gestión de Gestión de Seguridad de la Información (SGSI) para proteger sus activos más valiosos, estableciendo Politicas de Seguridad de la Información orientadas a garantizar la privacidad, integridad y accesibilidad de la información, estableciendo directrices y medidas para su manejo seguro y eficiente.

2. Objetivo de la Política

Gestionar de manera efectiva la seguridad de la información a lo largo de todo su ciclo de vida y en todos sus formatos mediante la aplicación rigurosa de normas y procedimientos estándar. Esto garantizará la preservación de la integridad, privacidad y disponibilidad de la información, tanto física como digital, dentro de la Empresa Pública Metropolitana de Servicios Aeroportuarios y Gestión de Zonas Francas y Regímenes Especiales (EPMSA).

2.1 Objetivos Específicos

Fortalecer la cultura organizacional en seguridad de la información, promoviendo de manera continua políticas, procedimientos, normas y buenas prácticas, para que todo el personal se mantenga informado y comprometido en la protección eficaz de la información.

Identificar y evaluar los riesgos de seguridad de la información para prevenir o mitigar posibles efectos negativos, implementando controles efectivos que permitan detectar vulnerabilidades de manera temprana y responder adecuadamente, asegurando la integridad, confidencialidad y disponibilidad de los datos.

Garantizar una gestión integral de incidentes de seguridad mediante un enfoque que incluya el análisis y la comunicación eficiente de eventos e incidentes, con procedimientos claros para su detección, evaluación y resolución, con el objetivo de minimizar su impacto en la institución.

3. Abreviaturas y Definiciones

3.1 Abreviaturas

- EPMSA. - Empresa Pública Metropolitana de Servicios Aeroportuarios y Gestión de Zonas Francas y Regímenes Especiales.
- ISO/IEC**. -** Comisión electrotécnica internacional y Empresa de normalización internacional.
- OACI. **-** Organización de Aviación Civil Internacional.
- EGSI. **-** Esquema Gubernamental de Seguridad de la Información.
- LOPDP**. -** Ley Orgánica de Protección de Datos Personales.

3.2 Definiciones

- Activo de información. - Es todo recurso tangible o intangible que tiene valor o significación.

- Autenticidad. **-** Implica garantizar que las personas, entidades o procesos sean los propietarios originales de un activo de información.

- Autorización**.** - Es permitir que alguien, algo o algún proceso acceda a un activo de información.

- Adaptabilidad. - Permite la identificación y el seguimiento de cualquier acción realizada por el usuario dentro de un sistema informático.

- Archivos. - Es un grupo de información o instrucciones que se guardan en un disco duro u otro medio de almacenamiento y se les da un nombre.

- Backup. - Para proteger de riesgos potenciales, se hace copias de la información y se las guarda de forma segura.

- Ciberamenazas. **-** Usar una red, un teléfono u otra tecnología telemática para amenazar a otra persona con daño grave a sí misma o a su familia con el fin de intimidarla.

- Confidencialidad. **-** Implica garantizar que las personas que no están autorizadas no puedan acceder al activo de información ni distribuirlo.

- Confiabilidad**.** - La información debe ser adecuada para la administración y cumplimiento de obligaciones de la entidad.

- Contraseña**.** - Es la clave de acceso a un terminal u ordenador personal, a un punto de la red, a un programa o secciones de un determinado programa, etc. Esta clave debe ser única, intransferible y no almacenada en ningún documento físicamente accesible.

- Cuenta de Usuario**.** - Es el identificador que utiliza un sistema de información para verificar la identidad de un usuario.

- Cuenta de Correo. - Servicio en línea que ofrece una ubicación para la recepción, transmisión y almacenamiento de mensajes electrónicos a través de Internet.

- Disponibilidad**.** - Implica asegurarse de que el activo de información esté disponible y accesible cuando lo necesiten personas, grupos o procesos.

- Eficiencia. - Utilizando la menor cantidad de recursos y el tiempo de respuesta más rápido posible, el procesamiento y suministro de información debe cumplir con este criterio de calidad.

- Equipos de cómputo. - Procesamiento de datos con equipo electrónico. Además, se consideran hardware de computadora que ofrece procesamiento y almacenamiento basados en la nube.

- Hardware. - Componentes de un sistema de procesamiento de datos en forma física.

- Integridad. **-** Consiste en asegurar o proteger la exactitud, precisión, consistencia, confiabilidad e integridad del activo de información.

- Incidente. - Es el acceso, intento de acceso, uso, divulgación, modificación o eliminación no autorizada de información.

- Información. - Es una colección estructurada de datos procesados que modifica el conocimiento del sujeto por parte del receptor o del sistema.

- Incidente de Tecnologías. - Cualquier acción que viole o intente violar las Tecnologías de la Información y las Comunicaciones (TIC), independientemente de la información que se dañe, la plataforma tecnológica utilizada, la frecuencia, los resultados, las ocasiones en que se hayan producido o su fuente, ya sea interna o externa.

- Ley Orgánica de Protección de Datos Personales (LOPDP).- Busca proteger a los propietarios de datos para que tengan control sobre quién recibe su información personal porque tienen fe en los proveedores de servicios digitales.

- No Repudio. - Es asegurarse de que ningún evento o transacción exigida por individuos, entidades o procesos resulte en la denegación del activo de información.

- Red. - Nombre que se le da al conjunto de equipos informáticos y de telecomunicaciones interconectados que utiliza la empresa para facilitar el acceso de los usuarios a los recursos tecnológicos.

- Software. - Un grupo de aplicaciones que permiten a las computadoras realizar tareas específicas.

- Vulnerabilidad. - La información se puede salvaguardar y proteger gracias a una combinación de medidas proactivas y reactivas.

4. Problemática

En la era digital, la seguridad de la información es esencial para la viabilidad y el éxito de las organizaciones. A medida que la dependencia de los datos almacenados en sistemas informáticos para la toma de decisiones en empresas, entidades gubernamentales y otros contextos organizacionales aumenta, surgen diversos desafíos.

La información puede presentarse en múltiples formatos, como impresos, electrónicos, grabaciones de voz, correos de voz o correos electrónicos. Sin importar el formato, método de entrega o almacenamiento, es crucial que esta información esté debidamente protegida.

La seguridad de la información tiene la responsabilidad de proteger estos datos contra amenazas, garantizando así la continuidad del negocio, reduciendo riesgos y maximizando el retorno de la inversión. Afortunadamente, las organizaciones son cada vez más conscientes del valor y la vulnerabilidad de sus activos en términos de

seguridad. En la actualidad, asegurar la información es vital para mantener la competitividad, la eficiencia, el cumplimiento de las normativas legales y una adecuada gestión del mercado en los sectores público y privado.

5. Justificación

En 2022, EPMSA enfrentó un incidente significativo que resultó en la pérdida de datos financieros, imágenes e información, así como en la necesidad de realizar una reprocesamiento constante de datos. Este evento subraya la importancia crítica de la información como un activo valioso para la empresa, lo que requiere la implementación de medidas estrictas para garantizar que los datos sean fiables, completos y actualizados de manera continua.

Para proteger este valioso activo, es fundamental salvaguardar los sistemas informáticos, los datos y la infraestructura frente a una amplia gama de amenazas, que incluyen fraude, sabotaje, espionaje industrial, chantaje, invasión de la privacidad, accesos no autorizados, ciberataques, interrupciones operativas, accidentes y desastres naturales. La protección integral de la información es clave para evitar daños a la seguridad, la reputación y la operación de la empresa.

6. Marco Jurídico

6.1. Ley de Protección de Datos Personales

La protección de datos personales (LOPDP) en Ecuador se reconoce desde 2008 a través de la Constitución de la República del Ecuador. Este derecho fundamental se ha fortalecido y regulado más específicamente con la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada el 26 de mayo de 2021.

La LOPDP establece un marco legal detallado para la protección de datos personales, aplicable tanto a organizaciones privadas como a entidades e instituciones del sector público. Esta ley regula de manera exhaustiva cómo se deben manejar, procesar y proteger los datos personales, asegurando que tanto el sector público como el privado cumplan con las obligaciones establecidas para salvaguardar la privacidad y los derechos de los individuos.

6.2. Ley Orgánica para la transformación digital y audiovisual

La Ley Orgánica para la Transformación Digital y Audiovisual de Ecuador, aprobada el 13 de diciembre de 2023, tiene como objetivo principal modernizar el sector digital y audiovisual del país.

Esta legislación establece un marco normativo que promueve la inversión en tecnología, favorece la producción audiovisual nacional y regula el entorno digital. A través de la mejora de la infraestructura tecnológica, se busca impulsar la innovación y fortalecer el desarrollo de nuevos contenidos y plataformas. Además, la ley garantiza la protección de los derechos digitales, asegurando un entorno seguro y transparente para los usuarios y los actores del sector.

6.3. Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024

El Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024, publicado el 27 de enero de 2024 en Ecuador, establece directrices para garantizar la protección de la información en la implementación de redes 5G. Define requisitos de seguridad específicos que las empresas deben cumplir para asegurar la confidencialidad, integridad y disponibilidad de los datos transmitidos.

El acuerdo tiene como objetivo mitigar los riesgos relacionados con la seguridad de la información, implementando medidas preventivas para enfrentar amenazas y vulnerabilidades en las infraestructuras de telecomunicaciones.

6.4. Organización de Aviación Civil (OACI), Anexo 17 “Seguridad de la Aviación”

Normativa establecida por la Organización de Aviación Civil (OACI) en el Anexo 17 “ Seguridad de la Aviación” Capítulo 4 Medidas Preventivas de Seguridad, numeral 4.9 Medidas relativas a las ciberamenazas, *“[…] 4.9.1 Cada estado contratante se asegurará de que los explotadores o entidades definidas en el programa nacional de seguridad de la aviación civil u otra documentación nacional pertinente identifiquen sus sistemas de tecnología de la información y las comunicaciones y datos críticos que se emplean para los fines de la aviación civil, y en función de una evaluación de riesgos elaboren y lleven a la práctica las medidas que correspondan para protegerlos de actos de interferencia ilícita.[…]”.*

El numeral 4.9 del Capítulo 4 del Anexo 17 de la Organización de Aviación Civil Internacional (OACI), titulado "Medidas relativas a las ciberamenazas", se enfoca en la protección de la aviación frente a amenazas cibernéticas.

Esta normativa establece que los Estados deben implementar medidas preventivas para proteger sus sistemas de información y redes contra ataques cibernéticos. Las medidas incluyen la evaluación de riesgos cibernéticos, la implementación de controles de seguridad, la capacitación del personal y la creación de protocolos para la gestión de incidentes cibernéticos. El objetivo es asegurar la integridad y la disponibilidad de los sistemas críticos de aviación para garantizar la seguridad operativa.

6.5. Esquema Gubernamental de Seguridad de la Información EGSI V3

El Esquema Gubernamental de Seguridad de la Información en Ecuador, vigente desde el 6 de febrero de 2023, establece un marco normativo para la protección de la información en el sector público. Su objetivo es asegurar la confidencialidad, integridad y disponibilidad de los datos en las instituciones gubernamentales.

El esquema define requisitos de seguridad, medidas preventivas y procedimientos para gestionar riesgos, así como para responder de manera efectiva a incidentes de seguridad.

6.6. Normas Técnicas ISO/IEC 27000

Para el desarrollo de nuestras políticas de seguridad de la información, adoptamos los estándares internacionales ISO 27001/2022, ISO 27002/2022 e ISO 27005/2022, los cuales abordan de manera integral la gestión de la seguridad de la información.

- **ISO 27001/2022** establece los requisitos necesarios para crear, implementar y mantener un sistema de gestión de seguridad de la información (SGSI), enfocado en garantizar la confidencialidad, integridad y disponibilidad de los datos en todas sus fases.
- **ISO 27002/2022** proporciona directrices y mejores prácticas para la implementación de controles específicos que respaldan la gestión y mitigación de riesgos en la seguridad de la información, complementando de manera efectiva a la ISO 27001.
- **ISO 27005/2022** se enfoca en la gestión de riesgos relacionados con la seguridad de la información, proporcionando un enfoque sistemático para identificar, evaluar y tratar dichos riesgos.

Estos estándares forman la base para garantizar que nuestras políticas de seguridad sean robustas, efectivas y alineadas con las mejores prácticas internacionales, lo que nos permite proteger adecuadamente la información y mitigar los riesgos asociados.

6.7. Reglamento de Administración de Talento Humano de la EPMSA

La norma administrativa tiene como objetivo regular el sistema de administración del talento humano dentro de la empresa, estableciendo los mecanismos para el ingreso, ascenso, promoción, régimen disciplinario, vacaciones y remuneraciones de los servidores públicos.

Esta norma está orientada a fomentar el desarrollo profesional, técnico y personal de los empleados, asegurando una gestión eficiente y alineada con los objetivos institucionales. Su implementación busca promover un entorno de trabajo que favorezca el crecimiento continuo de los colaboradores, contribuyendo a la mejora del desempeño y a la sostenibilidad organizacional.

7. Política de Seguridad de la Información

La información gestionada por EPMSA es muy importante para tomar decisiones sobre mejoras operativas. Para asegurar su confidencialidad, integridad y accesibilidad, los servidores encargados de la información deben seguir las directrices de este manual.

Basándose en la Norma ISO 27001:2022 se han establecido políticas de seguridad de la información para EPMSA, las cuales son flexibles y pueden modificarse siempre que no comprometan la seguridad. Los responsables de la seguridad de la información tienen la autoridad para implementar o ajustar estas políticas, que detallan componentes específicos y políticas adicionales que deben alinearse con las normas de control y las políticas organizacionales de EPMSA.

7.1 Descripción de la Política

El objetivo de la política de seguridad de la información es salvaguardar la integridad, confidencialidad y disponibilidad de los datos críticos, minimizando riesgos y garantizando un entorno seguro.

La Gerencia General de EPMSA reconoce la importancia de una gestión efectiva de la información, comprometiéndose a implementar un sistema integral de gestión de seguridad alineado con la misión y visión de la organización.

Este sistema tiene como propósito reducir los riesgos y mantener un nivel adecuado de exposición para proteger los activos institucionales y garantizar la seguridad de la información. La política aplica a todos los actores vinculados a la empresa, incluidos funcionarios, terceros, proveedores y la ciudadanía, asegurando el cumplimiento de los estándares para un manejo adecuado y seguro de la información.

7.2 Declaración de los Objetivos de Seguridad de la Información

a. Fortalecimiento de la cultura de seguridad

Promover y mantener prácticas de seguridad de la información a través de capacitación continua y la integración de estas prácticas en las actividades diarias para asegurar que todos los miembros adopten medidas proactivas.

b. Identificación de riesgos

Realizar una planificación y evaluación exhaustiva para anticipar y mitigar los riesgos de seguridad mediante la implementación de controles específicos, garantizando así una protección efectiva de la información.

c. Gestión de incidentes

Adoptar un enfoque integral para la gestión de incidentes de seguridad, que incluya integración de procesos, análisis detallado de eventos y comunicación efectiva sobre debilidades para minimizar su impacto negativo y asegurar una respuesta eficiente.

8. Roles y Responsabilidades

La implementación de las políticas de seguridad de la información es esencial para EPMSA. Con el fin de garantizar su correcta aplicación, se definen las siguientes responsabilidades:

a. *Gerencia General*

La Gerencia General de EPMSA debe proporcionar apoyo y recursos necesarios para la correcta implementación de las políticas de seguridad de la información, asegurando su integración efectiva en todos los aspectos operativos de la organización.

b. *Comité de Seguridad de la Información*

El Comité de Seguridad de la Información es responsable de revisar y actualizar las políticas de seguridad de la información de forma periódica. Esta revisión tiene como objetivo incorporar mejoras necesarias y adaptar las políticas a nuevos desafíos o cambios en el entorno operativo.

c. *Oficial de Seguridad de la Información*

El Oficial de Seguridad de la Información tiene la responsabilidad:

- Supervisar el cumplimiento de las políticas de seguridad dentro de la organización, lo que incluye monitorear al personal para garantizar que sigan las directrices establecidas.
- Brindar asistencia y resolver problemas relacionados con la seguridad cuando sea necesario, asegurando que se mantenga un entorno seguro y conforme a las normativas.
- Realizar verificaciones periódicas para asegurarse de que las políticas de seguridad se implementen de manera efectiva.
- En coordinación con Comunicación Institucional de la EPMSA es responsable de difundir la política de Seguridad de la Información, asegurando que todos los servidores de EPMSA reciban y comprendan la información necesaria para cumplir con las directrices y mantener altos estándares de seguridad.

d. *Usuarios y Proveedores*

La Política de Seguridad de EPMSA aplica a servidores de la empresa, proveedores, contratistas y usuarios externos. Los servidores deben conocer y reportar incidentes, los proveedores y contratistas deben cumplir con las políticas a través de acuerdos contractuales, y los usuarios externos deben adherirse a las políticas al interactuar con los sistemas y datos. Todos deben seguir la política para garantizar la protección de la información y el cumplimiento de los estándares de seguridad en EPMSA.

9. Alcance y Usuarios

La Política de Seguridad de la Información de EPMSA cubre todos los aspectos de protección y manejo de información dentro de la organización, incluyendo:

a. Áreas y Recursos

- Sistemas Informáticos: Hardware y software utilizados para procesar, almacenar y transmitir información.
- Datos y Documentación: Información en formatos digitales y físicos.
- Infraestructura: Instalaciones físicas y lógicas como redes, servidores y sistemas de almacenamiento.
- Procesos y Procedimientos: Gestión de incidentes, evaluación de riesgos y procedimientos de respuesta.

b. Tipos de Información

- Información Sensible: Datos críticos como información financiera y secretos comerciales.
- Información Confidencial: Información protegida para evitar accesos no autorizados.
- Información Pública: Datos que pueden ser divulgados sin comprometer la seguridad, pero deben manejarse responsablemente.

c. Usuarios de la Política

- Servidores de EPMSA: Deben conocer, seguir la política y reportar incidentes.
- Proveedores y Contratistas: Deben cumplir con las políticas de seguridad mediante acuerdos contractuales.
- Usuarios Externos: Deben adherirse a las políticas al interactuar con los sistemas y datos de la EPMSA.

Todos estos grupos deben seguir la política para proteger la información y asegurar el cumplimiento de los estándares de seguridad en EPMSA.

10. Comunicación de la Política

La comunicación y difusión de la Política de Seguridad de la Información a todos los servidores de EPMSA la llevará a cabo la Unidad de Comunicación Institucional de la EPMSA mediante una combinación de métodos y canales para asegurar que cada servidor esté debidamente informado y capacitado. Los procedimientos específicos para esta comunicación son los siguientes:

- Talleres y Capacitación

En coordinación con Comunicación Institucional de la EPMSA se organizarán talleres y sesiones de inducción en la seguridad de la información para todos los servidores.

Estos eventos proporcionarán una explicación detallada de la política, su importancia, y cómo se aplica en las actividades diarias. Estos talleres también ofrecerán la oportunidad para resolver dudas y recibir capacitación práctica.

La Comunicación se la realizará mediante:

a. Correo Electrónico

Se enviarán comunicaciones formales a través del correo electrónico a todo el personal. Estos mensajes incluirán el documento completo de la política, resúmenes clave y enlaces a recursos adicionales. Los correos electrónicos servirán para asegurar que cada empleado reciba la información directamente en su bandeja de entrada.

b. Volantes y Material Impreso

Se distribuirán volantes y otros materiales impresos en áreas comunes de la oficina. Estos documentos destacarán los aspectos más importantes de la política y estarán diseñados para facilitar su consulta rápida.

c. Portal Web

La política de seguridad de la información estará disponible en el portal web interno de EPMSA. Se proporcionará acceso fácil a través de un área dedicada en el portal, donde los servidores podrán consultar el documento completo y cualquier actualización relacionada.

d. Otros Medios

Se evaluarán y utilizarán otros canales de comunicación según sea necesario, como reuniones de equipo, boletines internos y presentaciones en eventos corporativos, para reforzar la comprensión y cumplimiento de la política.

Todo el personal de EPMSA tiene la obligación de conocer, aceptar y seguir las políticas descritas en este documento. El incumplimiento de estas políticas se considerará un incidente de seguridad, y dependiendo de la gravedad y las circunstancias del caso, podrá resultar en la implementación de un procedimiento disciplinario interno para los servidores afectados.

11. Excepciones y Sanciones

En ciertos casos específicos, la Política de Seguridad de la Información de EPMSA puede no ser aplicable. Las excepciones se definen a continuación:

a. Excepciones en cumplimiento de la Política de Seguridad de la Información

- Excepciones por Requerimientos Legales o Regulatorios

En situaciones donde leyes o regulaciones locales, nacionales o internacionales requieran excepciones a las políticas establecidas para cumplir con requisitos legales específicos, tales excepciones serán aceptadas siempre y cuando se justifiquen adecuadamente y se documente el cumplimiento con dichas leyes o regulaciones.

- Excepciones para Proyectos Especiales

En casos de proyectos especiales o iniciativas que requieran desviaciones temporales de la política para propósitos específicos y previamente autorizados por la Gerencia General o el Comité de Seguridad de la Información, se podrán otorgar excepciones. Estas deben ser documentadas y evaluadas para asegurar que no comprometan la seguridad de la información.

- Excepciones por Limitaciones Técnicas

Si existen limitaciones técnicas que impiden la implementación completa de ciertos aspectos de la política, se podrán considerar excepciones. Estas limitaciones deben ser justificadas y revisadas para garantizar que se implementen medidas compensatorias adecuadas para mantener la seguridad.

- Excepciones para Usuarios Externos

En situaciones donde contratos con proveedores o socios externos estipulen condiciones distintas a las políticas internas, las excepciones serán permitidas solo si están formalmente documentadas y aprobadas. Estas excepciones deben cumplir con los requisitos de seguridad establecidos en los contratos.

b. Sanciones por Incumplimiento de la Política de Seguridad de la Información

Las sanciones disciplinarias a cualquier violación de la presente Política de Seguridad de la Información pueden resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el reglamento de administración de talento humano de la EPMSA.

Es responsabilidad de todos los funcionarios notificar al responsable de Seguridad de la Información cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

- Acciones Correctivas

Las acciones correctivas incluyen la reparación de incidencias, donde el responsable del incumplimiento deberá colaborar en la corrección de daños, vulnerabilidades y la implementación de medidas correctivas. Además, se podrá requerir capacitación adicional para el personal involucrado, con el fin de garantizar una mejor comprensión y adherencia a las políticas de seguridad.

- Sanciones Contractuales

En caso de incumplimiento por parte de proveedores o contratistas, se podrán imponer sanciones contractuales que incluyen la terminación del contrato y reclamaciones por daños y perjuicios según los términos acordados.

- Acciones Legales

En situaciones donde el incumplimiento resulte en daños significativos o violaciones graves, EPMSA se reserva el derecho de tomar acciones legales para proteger sus intereses y recuperar cualquier pérdida.

La Política de Seguridad de la Información de EPMSA establece directrices para la gestión, protección y uso adecuado de la información, asegurando su integridad,

disponibilidad y confidencialidad. Aplica a empleados, contratistas y colaboradores, y clasifica la información en pública, interna y confidencial, con roles y permisos de acceso definidos.

Se implementarán protocolos para proteger datos personales, se prohibirá el uso no autorizado de la información y se establecerán procedimientos para manejar incidentes de seguridad. La política se ajustará a la normativa vigente, se revisará periódicamente y fomentará una cultura de seguridad y responsabilidad para proteger los intereses de EPMSA y sus usuarios.

12. Documentos de Referencia

- Ley Orgánica de Protección de Datos Personales.
- Ley Orgánica para la Transformación Digital y Audiovisual.
- Organización de Aviación Civil (OACI), Anexo 17 “Seguridad de la Aviación.”
- Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024.
- Esquema Gubernamental de Seguridad de la Información.
- Normas Técnicas ISO/IEC 27000.