GD-D11
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Versión 4
Fecha de aprobación 2026-07-01

ISES
SOLUCIONES ESPECIALIZADAS

ELABORADO POR:	REVISADO POR:	APROBADO POR:
<Líder de Seguridad y Ciberseguridad>	<Gerente de TI> <Coordinador de Calidad>	<Gerente General>
<DIANAL>	<CAVENIA> <MARIC>	<GGARCIA>

CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
1	Documento nuevo	2021-11-23
2	Se actualiza el nombre del documento, incluyendo el término de Ciberseguridad. Se adicionan directrices de ciberseguridad a lo largo del documento, se modifica declaración incluyendo lineamientos asociados a privacidad de la información y ciberseguridad. Se incluye ítem de directrices y mención de los dominios de seguridad aplicables al SGSI. Se incluye ítem de cumplimiento de la Política.	2024-02-06
3	Se actualiza la política modificando el apartado 2. Alcance en el cual se amplía el rango de aplicación de la política, se incluye mención de su publicación y revisión; se actualiza apartado 3. Definiciones, se elimina apartado de condiciones generales y se incluyen algunas de ellas en el nuevo apartado 6. Principios de la seguridad de la Información, se modifica apartado Declaración y se renombra a apartado 4. Compromiso de la Alta dirección, en este se eliminan los principios de seguridad que se llevan con mayor amplitud al apartado específico para ello, se adiciona apartado 5. Objetivos de Seguridad de la Información. Se modifica apartado 6 Principios de seguridad de la información, únicamente se relacionan principios de enfoque estratégico. Se elimina apartado: Directrices y dominios de la política de seguridad de la información. Se elimina apartado: Cumplimiento de la política de seguridad de la información y ciberseguridad porque esto pasa al Alcance. Se incluye aprobación y firma de la Política por parte de la Alta Dirección	2025-07-17
4	Se actualiza cargo de quien elabora el documento: Líder de Seguridad y Ciberseguridad. En apartado 2. Alcance se actualiza a personal que además custodien o interactúen con la información corporativa; se cita delimitación operativa y técnica del Sistema descrita en el Manual del SGSI, así como su alineación a	2026-07-01

	la norma ISO 27001; se adiciona mejora continua en la posición de la administración de la Empresa; y se extraen de este apartado los aspectos de publicación, actualización e incumplimiento reubicándolos en dos nuevos apartados del documento. En apartado 3. Definiciones se incluye definición de Seguridad de la Información y de SGSI. En apartado 4. Compromiso de la alta dirección, se incluye el compromiso con la mejora continua del SGSI; se amplía cumplimiento a regulatorio y contractual; se incluye concordancia también a objetivos y modelo de negocio de la empresa; y se mencionan amenazas emergentes asociado a la protección de la información. En apartado 5. Objetivos de seguridad de la información, se incluye mención de documento GD-D04 Objetivos y Metas del SIG. Se crea nuevo apartado 7. Roles y Responsabilidades. Se crea nuevo apartado 8 Revisión y vigencia, en el cual se reubican los aspectos de publicación y actualización; se incluyen responsabilidades asociadas a la gestión, validación y aprobación de la Política; y ejecución de auditorías internas al SGSI. Se crea nuevo apartado 9. Cumplimiento y Excepciones, en el cual se reubica directriz sobre incumplimiento de la política y se adiciona mención de excepciones. Se actualiza el Anexo A. Modelo de Política de seguridad y ciberseguridad que contiene la declaración para publicación física.	

UBICACIÓN
http://sig.ises.com.co/sig4/

TABLA DE CONTENIDO

1 OBJETO

Esta Política establece las directrices de seguridad y privacidad de la información, y ciberseguridad, para la protección de los activos de información de ISES, preservando la confidencialidad, integridad y disponibilidad de estos, bajo normativas y/o marcos de trabajo que apoyan la gestión y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI).

2 ALCANCE

Esta Política es de cumplimiento obligatorio para todos los empleados, contratistas, proveedores, practicantes y terceros que tengan acceso, custodien o interactúen con la información corporativa y los activos tecnológicos de ISES S.A.S., independientemente de su cargo, área funcional o modalidad de vinculación con la organización.

La delimitación operativa y técnica del Sistema de Gestión de Seguridad de la Información (SGSI) se detalla de manera específica en el documento ***TI-MP01 Manual del SGSI***, el cual también incluye los roles asociados al Sistema, establece las políticas complementarias de seguridad de la información y controles alineados a la Norma Técnica Colombiana NTC-ISO/IEC 27001:2022 y constituye el marco operativo que desarrolla los lineamientos de esta Política.

Esta Política representa la posición de la administración de ISES S.A.S, con respecto a la protección de los activos de información (registros, procesos, tecnologías de información incluido el hardware y el software), que soportan los procesos de la Empresa y apoyan la implementación, sostenibilidad y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), además de los requisitos legales y de otra índole asociados, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

3 DEFINICIONES

- **Activo de información:** Cualquier información o elemento relacionado con el tratamiento de esta que tenga valor para la organización.
- **Alta Dirección:** Persona o grupo de personas que dirigen y controlan al más alto nivel la Organización.
- **Ciberseguridad:** Conjunto de prácticas, tecnologías y políticas diseñadas para proteger sistemas, redes, programas y datos contra ataques cibernéticos, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información.
- **Ciberespacio:** Entorno digital interconectado conformado por sistemas de información, redes, dispositivos y servicios tecnológicos sobre los cuales se realizan las operaciones del negocio.
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Evento disruptivo:** Suceso imprevisto o no deseado que puede afectar la seguridad de la información, comprometiendo la confidencialidad, integridad o disponibilidad de esta.
- **Incidente de Seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Cualquier tipo de dato que tiene valor para una organización, independientemente de su formato (electrónico, papel, etc.) y de cómo se almacena o transmite.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Parte interesada:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de Continuidad de Negocio:** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Privacidad de la información:** El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la Empresa, en el marco de las funciones que a ella le compete realizar o servicios prestados, y que generan la correlativa obligación de proteger dicha información en observancia del marco legal.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.
- **Sistema de Gestión de la Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

4 COMPROMISO DE LA ALTA DIRECCIÓN

La Gerencia de ISES S.A.S, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), que involucra la privacidad de la información y ciberseguridad, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y la promesa de valor hacia sus partes interesadas; todo enmarcado en el cumplimiento legal, regulatorio y contractual, y en concordancia con la misión, visión, objetivos y el modelo de negocio de la Empresa.

Para ISES S.A.S, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos y amenazas emergentes identificados de manera sistemática, con objeto de mantener un nivel de exposición que permita responder por la confidencialidad, integridad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés.

Con respecto a la privacidad de la información, ISES S.A.S implementa los procesos y controles necesarios para el cumplimiento de las normativas legales aplicables, procurando la seguridad en la recopilación y el uso de los datos personales a nivel interno y de aquellos que conforman sus diferentes servicios. La privacidad de los datos abarca los mecanismos y protocolos para su correcto uso incluyendo aspectos tales como: el consentimiento, derechos de los usuarios según lo dictado por el gobierno nacional, el intercambio seguro de información y los canales de notificación.

Asimismo, para ISES S.A.S es un compromiso fundamental la protección de la información y de la infraestructura que la sustenta, con el fin de preservar la confidencialidad, integridad y disponibilidad de los procesos y la prestación de los servicios. Lo anterior mediante la implementación de estrategias y medidas de gestión en función del nivel de riesgo cibernético, integrando a los diferentes grupos de interés, los planes de negocio y los recursos tecnológicos necesarios para la defensa de su ciberespacio.

5 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información y Ciberseguridad de ISES S.A.S establece un marco estratégico que permite proteger de forma eficaz los activos de información y generar confianza entre las partes interesadas. En este sentido, se establecen los siguientes objetivos de seguridad de la información:

1. Desarrollar, establecer y mantener actualizadas las políticas y procedimientos del Sistema de Gestión de Seguridad de la Información, procurando su cumplimiento en todos los niveles de la organización.
2. Gestionar oportunamente los riesgos de seguridad de la información en el SGSI mediante la definición, evaluación periódica y seguimiento de los planes de tratamiento de riesgos.
3. Garantizar la atención oportuna de los incidentes de seguridad de la información, que permitan minimizar el impacto y mejorar la capacidad de respuesta del SGSI.
4. Fortalecer la capacidad de recuperación tecnológica de la organización mediante la planificación, ejecución y mejora continua de pruebas de contingencia, con el fin de asegurar la continuidad de las operaciones críticas del negocio ante escenarios de interrupción tecnológica.
5. Gestionar la implementación oportuna de remediaciones que minimicen la exposición a amenazas que comprometan la seguridad de la información.
6. Mantener los equipos de cómputo del negocio con soluciones antivirus actualizadas y operativas, asegurando la defensa proactiva contra amenazas y la integridad de los datos.
7. Clasificar, tratar y proteger la información de acuerdo con su nivel de sensibilidad y criticidad conforme a las disposiciones legales vigentes y los lineamientos internos.
8. Fomentar una cultura organizacional de seguridad y ciberseguridad, promoviendo la concientización, formación y compromiso de los empleados, practicantes, contratistas, proveedores y clientes de ISES S.A.S. y sus consorcios.
9. Consolidar y mantener la confianza de clientes, aliados, empleados y otras partes interesadas, a través del manejo seguro y responsable de la información.

Los indicadores de medición, metas, frecuencia y responsables se documentan en ***GD-D04 Objetivos y Metas del SIG.***

6 PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

INGENIERIA Y SOLUCIONES ESPECIALIZADAS S.A.S. establece las políticas de seguridad que sustentan su Sistema de Gestión de Seguridad de la Información (SGSI) y se compromete a:

1. Establecer, implementar, operar, mantener y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información conforme a las necesidades del negocio, los requisitos de las partes interesadas y las obligaciones legales, contractuales y regulatorias aplicables a su actividad.

2. Definir y asignar responsabilidades claras en materia de seguridad de la información, comunicadas y aceptadas por todos los empleados, socios de negocio, contratistas, proveedores, y terceros que interactúen con los activos de información de ISES S.A.S.

3. Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales aplicables en materia de seguridad de la información y protección de datos.

4. Fortalecer la cultura organizacional en torno a la seguridad de la información y la ciberseguridad, a través de estrategias de formación y concientización dirigidas a todos los usuarios internos y externos (cuando aplique) con acceso a la información del negocio.

5. Asegurar la clasificación y protección de la información conforme a su nivel de sensibilidad y criticidad, aplicando controles adecuados que permitan prevenir impactos financieros, operativos, legales o reputacionales como consecuencia de su uso indebido o acceso no autorizado.

6. Garantizar la protección de la información y de los activos tecnológicos frente a accesos no autorizados, pérdida, alteración o divulgación indebida por parte del personal interno o terceros, conforme a los principios de confidencialidad, integridad, disponibilidad y cumplimiento de la normativa legal aplicable.

7. Implementar controles de seguridad física y lógica sobre la infraestructura tecnológica para asegurar la disponibilidad, integridad y confidencialidad de los procesos críticos del negocio.

8. Proteger los datos personales de empleados, clientes, contratistas, proveedores, aliados estratégicos y demás partes interesadas, a través del tratamiento adecuado de la información conforme a lo dispuesto en la normativa legal vigente de protección de datos personales.

9. Establecer y mantener un enfoque proactivo y eficaz para la supervisión, detección, gestión y respuesta ante incidentes de seguridad de la información, con el objetivo de minimizar impactos adversos y restablecer la operación normal en el menor tiempo posible.

10. Aplicar estrategias de continuidad del negocio y recuperación ante desastres que preserven la disponibilidad de los servicios y procesos críticos, permitiendo la continuidad operativa ante eventos disruptivos.

11. Integrar la seguridad de la información a lo largo de todo el ciclo de vida de los sistemas de información.

7 ROLES Y RESPONSABILIDADES

La Alta Dirección es la máxima responsable del cumplimiento de la presente Política, por lo tanto, asegura que las responsabilidades y autoridades para los roles del Sistema de Gestión de Seguridad de la Información (SGSI) sean asignadas y comunicadas, estos se citan en el documento ***TI-MP01 Manual del SGSI.***

8 REVISIÓN Y VIGENCIA

Esta Política será revisada al menos una vez al año, o cuando se presenten cambios significativos en el entorno interno o externo, con el fin de asegurar su vigencia, adecuación y mejora continua.

Cualquier modificación a esta Política, ya sea producto de la revisión periódica o de cambios significativos, será gestionada por el Líder de Seguridad y Ciberseguridad, validada por la Gerencia de TI y aprobada formalmente por la Alta Dirección antes de su publicación. La versión oficial y vigente para conocimiento del personal interno y de las partes interesadas, será la que se encuentre publicada en las plataformas corporativas autorizadas.

La Política será comunicada al personal interno a través del aplicativo interno definido para tal fin y para las partes externas estará disponible en la página web de ISES.

El Sistema de Gestión de Seguridad de la Información (SGSI) será evaluado mediante auditorías internas periódicas con el fin de verificar su conformidad, eficacia y cumplimiento frente a los requisitos de la Norma NTC-ISO/IEC 27001:2022 y los lineamientos internos.

9 CUMPLIMIENTO Y EXCEPCIONES

Las directrices establecidas en esta Política son de obligatorio cumplimiento por parte del personal y terceros relacionados con ISES S.A.S. El incumplimiento de esta Política podrá derivar en sanciones disciplinarias internas conforme a los reglamentos de ISES S.A.S., así como en consecuencias legales conforme a la normativa nacional vigente sobre seguridad de la información y protección de datos.

Cualquier excepción a las políticas de seguridad de la información deberá ser solicitada formalmente por el Gerente o Líder de área, a través del canal oficial de seguridad de la información para su evaluación, de acuerdo con el proceso operativo establecido en el documento ***TI-MP01 Manual del SGSI.*** Toda excepción aprobada estará sujeta a condiciones, plazos y controles compensatorios definidos.

10 ANEXOS

- TI-MP01 Manual del SGSI - Sistema de Gestión de Seguridad de la Información.
- GD-D09 Política de Tratamiento de Datos Personales.

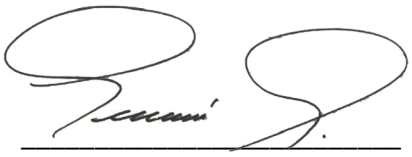
ANEXO A. MODELO DE POLÍTICA DE SEGURIDAD Y CIBERSEGURIDAD PARA PUBLICACIÓN FÍSICA

La Gerencia de ISES S.A.S, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), que involucra la privacidad de la información y ciberseguridad, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y la promesa de valor hacia sus partes interesadas; todo enmarcado en el cumplimiento legal, regulatorio y contractual, y en concordancia con la misión, visión, objetivos y el modelo de negocio de la Empresa.

Para ISES S.A.S, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos y amenazas emergentes identificados de manera sistemática, con objeto de mantener un nivel de exposición que permita responder por la confidencialidad, integridad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés.

Con respecto a la privacidad de la información, ISES S.A.S implementa los procesos y controles necesarios para el cumplimiento de las normativas legales aplicables, procurando la seguridad en la recopilación y el uso de los datos personales a nivel interno y de aquellos que conforman sus diferentes servicios. La privacidad de los datos abarca los mecanismos y protocolos para su correcto uso incluyendo aspectos tales como: el consentimiento, derechos de los usuarios según lo dictado por el gobierno nacional, el intercambio seguro de información y los canales de notificación.

Asimismo, para ISES S.A.S es un compromiso fundamental la protección de la información y de la infraestructura que la sustenta, con el fin de preservar la confidencialidad, integridad y disponibilidad de los procesos y la prestación de los servicios. Lo anterior mediante la implementación de estrategias y medidas de gestión en función del nivel de riesgo cibernético, integrando a los diferentes grupos de interés, los planes de negocio y los recursos tecnológicos necesarios para la defensa de su ciberespacio.



German Garcia Valenzuela
GERENTE GENERAL
Versión 4
Fecha de aprobación: 2026-07-01

Documento vigente publicado en la intranet. ISES S.A.S está comprometido con el medio ambiente, evite la impresión innecesaria. Cualquier documento impreso se considera copia no controlada.