SISTEMA INTEGRADO DE GESTIÓN

CONJUNTO POLÍTICAS TÉCNICAS SGSI

DOCUMENTO: SI-5-523-1225		
Elaborado por: Auxiliar Seguridad de Información	**Revisado Por:** Coordinador SIG / Director TIC's	**Aprobado Por:** Comité SI

TABLA CONTROL DE CAMBIOS

Versión	Resumen del Cambio	Fecha
1	Diseño del manual de procesos dirección de TIC's	01/2014
2	Actualización del manual de procesos dirección de TIC's	07/2016
3	Actualización del manual de procesos dirección de TIC's	03/2019
4	Integración de requisitos técnicos para el servicio soporte TIC's	31/07/2022
5	Ajuste de política de control de acceso a la información	24/05/2024
6	Actualización de políticas técnicas acorde a la ISO/IEC 27001:2022	10/01/2025
7	Inclusión de A.8.12 política de prevención de fuga/pérdida de datos aplicando la directiva específica sobre trasmisión de información secreta y/o sensible por correo Office 365. Actualización de A.5.12 política de clasificación de información y A.5.13 política de etiquetado de la información en Office 365.	31/07/2025
8	Inclusión del control A.5.31 Requisitos legales, legales, reglamentarios y contractuales, Política de uso Responsable y Ético de la Inteligencia Artificial (IA)	09/09/2025
9	Revisión anual y aprobación del SI-5-523- Conjunto de políticas técnicas SGSI por parte de la gerencia corporativa.	03/12/2025

Política Seguridad de la información

INGEOMEGA S.A.S es una empresa dedicada al desarrollo de operaciones y proyectos de ingeniería, eléctrica, civil, telecomunicaciones y gas combustible a nivel nacional. Reconocemos la información como un activo fundamental en nuestras operaciones y proyectos, nuestro compromiso se basa en garantizar su protección mediante altos estándares de seguridad de la información, satisfaciendo los requisitos aplicables con la seguridad de la información, alineado con los principios de la NTC-ISO/IEC 27001:2022, implementando medidas para proteger la confidencialidad, integridad y disponibilidad, satisfaciendo las necesidades y expectativas de nuestras partes interesadas y promoviendo la mejora continua en todos los procesos. Lo anterior lo logramos a través de:

- Establecer y mantener un entorno organizacional que promueva una cultura de seguridad de la información entre todas las partes interesadas.
- Implementar un proceso sistemático para identificar, evaluar y mitigar las vulnerabilidades que afectan la información de la organización, asegurando una respuesta ágil y adaptativa a las amenazas emergentes del entorno.
- Fomentar un ciclo de mejora continua en la implementación y desarrollo del SGSI, mediante la revisión regular de políticas, procesos y controles de seguridad.
- Establecer mecanismos de monitoreo efectivos para garantizar el cumplimiento de los requisitos legales y normativos aplicables en materia de protección de datos y seguridad de la información.
- Garantizar el monitoreo continuo y efectivo de la seguridad física de las instalaciones, permitiendo la detección oportuna y la respuesta ante incidentes de seguridad.

La organización está comprometida con la integración de la gestión del cambio climático y la sostenibilidad ambiental, considerándolo como una cuestión pertinente en el sistema de gestión de seguridad de la información.

Todos los niveles de la organización son responsables del cumplimiento y aplicación de esta política.

MARCO AURELIO VIEIRA MEJÍA
GERENTE GENERAL

Conjunto políticas técnicas SGSI

A.5.9. Política de uso de activos de información

Ingeomega S.A.S. está comprometida con la identificación, registro, gestión y protección de los activos de información y otros activos asociados, reconociéndolos como recursos esenciales para el soporte del negocio. Por esta razón, la organización establece que todos los activos deben son identificados, inventariados y clasificados de manera precisa y alineada con los niveles definidos en la política de clasificación de la información. Esta clasificación debe incluir no solo información, sino también hardware, software, equipos de procesamiento, bases de datos y almacenamiento.

La Dirección de TIC's es el responsable de la adquisición, uso, administración, mantenimiento y disposición del inventario centralizado y actualizado, el cual debe reflejar el tipo de activo, su ubicación, propietario, estado y cualquier componente asociado, como sistemas operativos, aplicaciones y dispositivos físicos.

Todos los activos asignados deben ser utilizados exclusivamente para fines laborales asociados a las funciones asignadas. No está permitido el almacenamiento de información corporativa en medios locales o dispositivos

personales no autorizados. Toda la información debe almacenarse en los sistemas designados por la organización, tales como NAS o servicios en la nube, en cumplimiento de los lineamientos establecidos en el SP-5-505- Manual de Almacenamiento en Medios Magnéticos.

A.5.10. Política de uso aceptable de la información y otros

Para garantizar que la información y otros activos asociados se protejan, utilicen y manejen adecuadamente, se establecen lineamientos que aseguren que los dispositivos asignados cuenten con protección contra programas maliciosos y configuraciones que garanticen la integridad y confidencialidad de la información, y en cumplimiento con la Ley de Protección de Datos Personales.
Queda expresamente prohibido almacenar información secreta o clasificada de Ingeomega S.A.S. en dispositivos no corporativos o en medios locales. Se implementarán mecanismos de desactivación remota en caso de pérdida o robo, análisis periódico mediante monitoreos de seguridad y auditorías de acceso conforme a lo establecido por el SGSI, así como el uso de conexiones seguras con configuraciones técnicas apropiadas. Asimismo, los equipos y recursos corporativos deberán emplearse exclusivamente para fines laborales y de acuerdo con los lineamientos de seguridad establecidos, protegiendo contraseñas y cuentas sin permitir su uso por terceros y respetando los procedimientos destinados a salvaguardar la información sensible de la empresa, sus socios y clientes.
Los mensajes de correo electrónico deberán enviarse únicamente a receptores autorizados, limitando el uso del correo corporativo y activos de la empresa a actividades permitidas, evitando la transmisión de materiales inapropiados, ilegales o discriminatorios, y reportando al SGSI cualquier incidente de seguridad, como accesos no autorizados, pérdida de dispositivos o posible compromiso de la información.
Se requiere autorización para el uso de equipos personales en actividades laborales, los cuales deben cumplir con los requisitos de seguridad establecidos por el SGSI, y toda información compartida con proveedores deberá contar con la autorización correspondiente. Además, está prohibido el manejo de contraseñas compartidas, la apertura de archivos provenientes de remitentes desconocidos, el uso de la misma clave en diferentes plataformas y el uso de los servicios de correo electrónico o activos de Ingeomega para descargar, almacenar o distribuir contenido que contenga material pornográfico, fomente la discriminación por etnia, sexo, nacionalidad, edad, estado civil, orientación sexual, religión o discapacidad, implique comportamientos amenazantes o violentos, se relacione con actividades ilegales o juegos de apuestas, o se refiera al reenvío de "cadenas" de correo electrónico.

A.5.12. Política de Clasificación de la información

Inventariados los activos de la información, se define como política de clasificación de la información los siguientes niveles: Personal – Secreto – Clasificado – Interno - Publico, los cuales determinaran el tratamiento, etiquetado y almacenamiento de la información digital y física. Con el fin de disminuir los riesgos a los que está expuesta la información se hace necesario que el propietario tenga la capacidad de clasificarla según los criterios definidos por SGSI, estos criterios están basados de acuerdo con requisitos legales, impacto, criticidad y susceptibilidad a divulgación o a modificación no autorizada. Los niveles de clasificación son los siguientes:

Personal: Este nivel aplica para información altamente sensible y de uso exclusivo del titular de la información. Su contenido incluye datos sensibles, privilegiados o íntimos, cuya divulgación, modificación o pérdida no autorizada puede generar graves consecuencias legales para el titular de la información como para la organización. El acceso, tratamiento, almacenamiento y eliminación es responsabilidad del titular de la información.

Secreto: Este nivel de clasificación se aplica a la información altamente sensible (datos personales, financieros y casos clínicos) y cuya divulgación podría causar un impacto a la organización y/o las personas. Esta información está protegida bajo los criterios definidos por el responsable o delegado

por la gerencia general para esta labor, y serán ellos quienes determinen la custodia divulgación y protección.

Nota: La organización se reserva el derecho de administrar y etiquetar la información física que la gerencia general determine como SECRETA, entendiendo que dicha reserva no deberá afectar e interferir en la dinámica SGSI

Clasificado: Información de interés para grupos delimitados de acuerdo con la estructura organizacional, procesos y/o proyectos. Este nivel de clasificación se aplica a la información que tiene una pertinencia particular y cuya divulgación afecta el desarrollo de los procesos y la operatividad de la organización.

Interno: Información de interés y transversal para todos los miembros dentro de la organización. Este nivel de clasificación se aplica a la información necesaria en la operación interna de la organización.

Público: Información de libre circulación e interés para la comunidad Este nivel de clasificación se aplica a la información que no tiene ninguna restricción de acceso y que puede ser divulgada de manera libre.

Criterios			
Requisitos legales	**Criticidad**	**Impacto**	**Susceptibilidad a divulgación o modificación no autorizada**
Cumplimiento de disposiciones legales, contractuales y regulatorias aplicables (Ley 1581, Ley 23, Habeas data)	Nivel de afectación en la continuidad, operatividad y disponibilidad de los proyectos o de los procesos asociados.	Afectación o impacto económico, legal, reputacional u operativa asociado a la pérdida de Disponibilidad, Confidencialidad y/o Integridad	Impacto generado por la divulgación, acceso, modificación o perdida no autorizada de información.

Tabla de valoración			
Criterio	**Valoración**	**Sumatoria**	**Clasificación**
Muy Alto	5	Mayor a 17 y menor o igual a 20	Personal
Alto	4	Mayor o igual a 13 y menor o igual a 16	Secreto
Medio	3	Mayor o igual a 9 y menor o igual a 12	Clasificado
Bajo	2	Mayor o igual a 5 y menor o igual que 8	Interno
Muy Bajo	1	Igual a 4	Publico

Responsabilidades	
Gerentes de procesos / áreas	Define las estrategias de clasificación y aprueba excepciones
Sistema de Gestión de Seguridad de la Información	Supervisa y audita la aplicación de la clasificación
Propietario de la información	Clasifica y revisa la información bajo su control
Usuarios	Respetar y aplicar la clasificación de uso diario de la información

A.5.13. Política de Etiquetado de la información

El etiquetado documentos, carpetas físicas o digitales, correo electrónico o cualquier información que se divulgue dentro y fuera de la organización se regirá por los parámetros de la política de clasificación de la información y será responsabilidad del propietario la clasificación y etiquetado, toda aquella información que no cuente con ningún etiquetado se considerará pública.

El etiquetado se hará mediante:

Etiquetado	
Archivos físicos	Se realizará mediante sellos, estos permitirán la marcación de la documentación para situaciones como: transporte de información fuera de la empresa o cuando requiera ser archivada, para este caso el lugar de almacenamiento deberá contar cerradura, y con la temperatura adecuada para la conservación de este y será la responsabilidad del director de área disponer del lugar.
Correo electrónico.	Teniendo en cuenta la política de clasificación de la información los correos se etiquetarán según los parámetros establecidos en esta, para los casos de información clasificada como **SECRETA** o **CLASIFICADA** se etiquetará, para los demás será decisión del dueño de la información si realiza el etiquetado.
Almacenamiento digital.	**Archivos propios:** Todo archivo debe de estar etiquetado con la clasificación llevando la palabra completa en marca de agua, para el caso de documentación clasificado como **PUBLICO** y **SECRETO** no será de obligatorio uso la etiqueta
	WEBSIG: Para el caso de los archivos, formatos, instructivos, procedimientos, manuales, políticas y demás archivos almacenados en dicho repositorio se etiquetera con marca de agua con la palabra completa, se entenderá que toda la documentación está clasificada como INTERNO **Nota:** Para el caso de los formatos que se convierten en registro se deberá realizar la clasificación de la información una vez estos queden diligenciados según lo establecido en la política de clasificación y política de etiquetado.
	NAS: Para el caso de los archivos almacenados en las NAS se etiquetará la carpeta madre con la Inicial del criterio correspondiente**.** Solo será etiquetados los archivos clasificados dentro de estas dos categorías para el caso de documentación clasificados como **PUBLICO** y **SECRETO** no será de obligatorio uso la etiqueta

Cada miembro de la organización es responsable almacenar su información en servidores, NAS o nube, toda la información almacenada de forma local es susceptible a pérdida y la dirección de TIC's, no se hará responsable de la pérdida de esta.

Nota: Los documentos que queden clasificados como **PUBLICOS y SECRETOS** se omite su etiquetado.

A.5.14 Políticas y procedimientos de transferencia de información

Está política, define los lineamientos y canales de tránsito de datos permitidos para llevar a cabo la emisión y recepción de información corporativa, a través de un conjunto de procedimientos y controles, cuyo objetivo es disminuir el riesgo de pérdida de integridad y confidencialidad en la información transmitida, además, Ingeomega establece acuerdos de confidencialidad donde se describe explícitamente la responsabilidad en la divulgación de la información.

- **Política de transferencia digital**

La difusión y transmisión de información usando canales de mensajería electrónica, se realizará a través de mecanismos implementados por la organización, los cuales deben garantizar que el activo utilizado como medio responda a las exigencias de confidencialidad e integralidad en la información del mensaje transmitido. Ingeomega podrá implementar mecanismos de autenticación adicionales si lo considera necesario. El correo electrónico corporativo es el único medio autorizado para transmisión de mensajes utilizando este servicio, las redes sociales oficiales serán administradas desde el área de comunicaciones. Cada correo electrónico tiene en su firma definida una marca de confidencialidad.

- **Política de transferencia física**

Solo se podrán compartir archivos a través de plataformas autorizadas por la Dirección TIC's a través del SGSI. Está prohibido transferir información clasificada en memorias USB o discos duros externos. Toda transferencia de información clasificada o secreta con proveedores debe estar respaldada por un acuerdo de confidencialidad firmado.

- **Política de transferencia verbal**

Toda información confidencial discutida debe ser documentada posteriormente mediante correo electrónico o acta. Se debe tener cláusula de confidencialidad en los contratos de trabajo de los empleados. Se debe evitar hablar sobre información corporativa en lugares públicos.

A.5.15. Política de control de acceso a la información.

Ingeomega S.A.S. reconoce la importancia y responsabilidad en la seguridad de la información gestionada y/o almacenada en sus activos. Bajo esta premisa, establece los lineamientos para el control de acceso a la información con el fin de administrar y conceder adecuadamente los accesos a la información, bien sea de forma física, determinados a más detalle en la sección G Seguridad física y del entorno**,** o de forma virtual, gestionando el control de contraseñas de activos de información, desde la creación de las cuentas de acceso hasta la desactivación de estas por medio del ciclo de vida de los usuarios.

- **Lineamientos para el control de acceso**

En alineación con el SI-5-512-Instructivo control de contraseñas activos de información, se establecen los lineamientos para la creación y gestión de contraseñas para el acceso a la información y los activos de Ingeomega S.A.S., son los siguientes:

1. Criterios para la creación de contraseñas:

Las contraseñas deben tener una longitud mínima de 12 caracteres, que incluyan:

- Dos letras en mayúscula (AZ).
- Cuatro números (0000-9999).
- Tres caracteres especiales (#, *, (,), “, $, ¿,', +, /, -).
- La cantidad de letras en minúscula que el usuario desea incluir (az).

Ejemplo: IngeOmega2024+/-

2. Criterios para contraseñas relacionadas con equipos y aplicaciones:

Longitud mínima de 12 caracteres, incluyendo:

- Una letra en mayúsculas (AZ).
- Números (0, 1, 2, 3, etc.).
- Caracteres especiales (#, *, (,), “, $, ¿,', +, /, -).
- Letras en minúscula según el criterio del usuario (az).

Ejemplo: Ingeomega2024*

Las contraseñas deben actualizarse cada 90 días como medida preventiva de seguridad.

Estos lineamientos buscan fortalecer la seguridad de los accesos y mitigar riesgos asociados al acceso no autorizado a los sistemas de información de la organización.

- **Política de suministro de accesos.**

Ingeomega S.A.S. reconoce la importancia de tener un control de todos los accesos que se tienen a los aplicativos, activos de la información y/o equipos críticos de procesamiento de información, por lo tanto, se definen procedimientos para el ciclo de vida de los accesos a la información.

- **Política de uso de la información.**

Conscientes de la importancia de la protección de la información, se establece y difunde ampliamente que todo individuo en vínculo con la organización como empleado, socio, contratista o proveedor es responsable de proteger la información, no divulgar las credenciales de acceso suministradas y mantener las buenas prácticas contenidas en el sistema SGSI. Toda pérdida o mal uso de la información que conduzca a situaciones como pérdida de confidencialidad e incumplimiento de regulaciones y leyes aplicables a la Organización, será su responsabilidad, y se procederá con el proceso disciplinario o legal correspondiente.

A.5.16. Política de gestión de identidad

El usuario y clave es individual y confidencial, es decir, los datos de acceso a los sistemas de información deberán estar compuestos por un nombre de usuario y una contraseña única con las funciones que necesita usar en el sistema cada colaborador o tercero. Los datos de acceso a los sistemas de información deberán estar compuestos por un nombre de usuario y una contraseña única por cada colaborador o tercero, el cual se hará responsable de las acciones realizadas con los mismos. Toda solicitud de creación y/o modificación de usuarios y/o perfiles de estos, deberá efectuarse por escrito a través de la plataforma OSTickets de Ingeomega. En dicha solicitud deben ser consignados los datos mínimos del requerimiento: nombre e identificación de la persona a la que se asignará el rol, nombre del rol y área funcional en la que requiere el mismo. Los detalles

para este procedimiento están detallados en el documento SP-5-503 Procedimiento Control de acceso a la información.

A.5.17 Política de información de autenticación

Todas las credenciales de acceso serán asignadas de manera segura y personalizada. Los sistemas deberán tener activado el forzado de cambio de Contraseña Inicial para exigir a los usuarios a cambiar su clave inicial asignada, previo al uso del sistema por primera vez. Los sistemas deberán tener activado el forzamiento de historial de contraseñas para que clave no puede ser igual a la clave anteriores. Las contraseñas y datos de autenticación no deben enviarse ni almacenarse en texto plano ni a través de canales inseguros como correos electrónicos.

A.5.18 Política de derechos de acceso

La asignación y uso de permisos de administrador y privilegios especiales estará restringida y controlada, debido a su alto impacto en la continuidad operativa de las plataformas tecnológicas. Todo acceso privilegiado debe otorgarse únicamente bajo autorización explícita del propietario del sistema y documentarse en el SGSI. Los accesos privilegiados deben estar sujetos a monitoreo y auditoría mediante verificación de registros de acceso y alertas de actividad sospechosa. Cuando se asigne un permiso sobre una plataforma/servicio, debe ser con autorización del propietario. El área de TIC's y SGSI supervisará el cumplimiento de la eliminación de accesos y documentará los procedimientos de revocación en la plataforma de gestión de tickets. En casos especiales donde se concedan permisos temporales a un sistema de información, deberá ser con la autorización del responsable, lo cual va acompañado siempre de una fecha de vencimiento. Los permisos o accesos deben ser solicitados por medio de la plataforma de os tickets por el líder de cada área.

- **Política de derechos de acceso físico**

Solo personal autorizado podrá acceder a áreas críticas como el centro de datos, servidores y salas de telecomunicaciones las cuales deberán contar con control de acceso seguro y que permita monitorearse. Los visitantes deben registrarse y contar con supervisión mientras permanezcan en instalaciones con acceso a información sensible.

- **Política de derechos de acceso lógico**

Los accesos privilegiados deben estar sujetos a monitoreo y auditoría mediante verificación de registros de acceso y alertas de actividad sospechosa. Cuando se asigne un permiso sobre una plataforma/servicio, debe ser con autorización del propietario. El área de TIC's y SGSI supervisará el cumplimiento de la eliminación de accesos y documentará los procedimientos de revocación en la plataforma de gestión de tickets. En casos especiales donde se concedan permisos temporales a un sistema de información, deberá ser con la autorización del responsable, lo cual va acompañado siempre de una fecha de vencimiento. Los permisos o accesos deben ser solicitados por medio de la plataforma de os tickets por el líder de cada área.

A.5.19 Política de seguridad de la información para las relaciones con proveedores

Los proveedores cuyas actividades contratadas involucren acceso a activos de información deberán ajustarse a la política de seguridad establecida por el SGSI, bajo los lineamientos definidos de control de acceso y las políticas asociadas al tratamiento y protección de la información, extendiendo los controles a escenarios de riesgo que comprometan su confidencialidad. Ingeomega S.A.S. limita al mínimo el alcance respecto al acceso a la información para los proveedores y contratistas. Todo acuerdo contractual deberá definir de manera explícita la responsabilidad de confidencialidad y el alcance de la sanción por su incumplimiento.

A.5.24 Política de *Help desk* (Mesa de Ayuda)

Se crea una mesa de ayuda con el objeto de proveer a los usuarios de sistemas de información, un punto único de contacto mediante el cual se resuelvan y/o canalicen requerimientos e incidentes de acuerdo con un estándar definido a través del análisis de riesgos y vulnerabilidades. De acuerdo con la dinámica de la organización, se requiere tener sistemas centralizados de atención apoyados en una plataforma de software web cuyas funciones específicas son:

- Recibir y atender las solicitudes de incidentes o requerimientos.
- Permitir al usuario y al agente realizar seguimiento en línea al caso generado.
- Documentar y anexar información adicional de usuarios, agentes.
- Generar indicadores de atención tanto del personal de la dirección como del Outsourcing
- Servir de base de conocimientos para resolver incidencias con base en lecciones aprendidas.
- Servir de base de conocimientos para resolver incidencias con base en lecciones aprendidas.
- Permitir al SGSI identificar los incidentes de seguridad para ser tratados por el comité de la información.

A.5.31 Requisitos legales, legales, reglamentarios y contractuales

Política de uso Responsable y Ético de la Inteligencia Artificial (IA)

1. **Objetivo** Establecer un marco de actuación para el uso de sistemas de Inteligencia Artificial (IA) en Ingeomega S.A.S., asegurando que su implementación se alinee con los principios éticos, requisitos legales como la ley 1581 de 2012, decreto 1377 de 2013, ley 2502 de 2025, circular 002 de 2024 y las que la complementen, el Sistema de Gestión de Seguridad de la Información (SGSI) y la política de privacidad, tratamiento y protección de datos personales de Ingeomega

2. **Alcance** Esta política aplica a todos los colaboradores en el marco de su rol, responsabilidades y funciones con Ingeomega S.A.S., tengan acceso, procesen, almacenen y/o utilicen sistemas de IA.

3. **Principios y Lineamientos de la Política**

Ingeomega S.A.S. se compromete a cumplir con los siguientes lineamientos, en concordancia con el Artículo 4° de la Ley 2502 de 2025:

1. **Marco Ético.** Ingeomega S.A.S. promueve el uso de la IA en un ecosistema digital que es inclusivo, confiable y sostenible. Todas las herramientas de IA utilizadas respetan la privacidad, dignidad humana y los derechos fundamentales. El tratamiento de datos a través de IA se regirá por los principios de legalidad, finalidad, transparencia, seguridad y confidencialidad establecidos en la política de privacidad, tratamiento y protección de datos personales de Ingeomega.

2. **Colaboración Intersectorial.** Se fomenta la colaboración entre las diferentes áreas de la organización (Dirección de TIC's, SIG, Talento Humano, entre otras.) y con actores externos como, entes reguladores y la sociedad civil. El objetivo es compartir conocimientos y estrategias para identificar de manera proactiva los riesgos asociados al uso de la IA, especialmente en lo que respecta a la suplantación de identidad personal y la afectación de derechos de autor.

- **Gestión del Conocimiento:** Los aprendizajes y buenas prácticas identificados en estos espacios serán compartidos internamente a través del canal del centro de Excelencia Copilot Ingeomega.

3. **Educación y Capacitación.** La organización implementa programas de formación y capacitación anual para todo el personal que utilice herramientas de IA. Esté programa tiene un enfoque en ciberseguridad como riesgos de seguridad (phishing, deepfakes), la política de clasificación y etiquetado de información, el uso de contraseñas seguras y el procedimiento de reporte de incidentes, además, principios éticos de la IA y el uso responsable de la tecnología. La participación en estas formaciones y capacitaciones son obligatorias para los colaboradores con licencias asignadas.

4. **Desarrollo y Adopción de Tecnología.** Ingeomega impulsa la innovación en IA confiable, evaluando las consecuencias sociales, jurídicas y éticas de su implementación. La Dirección de TIC's es responsable de investigar y adoptar herramientas de IA específicas, utilizando tecnologías avanzadas para proteger a la organización y a sus partes interesadas.

    - **Solicitud de Licencias:** Toda solicitud de una herramienta o licencia de IA debe realizarse a través de la plataforma de tickets (OSTickets), con la aprobación del jefe inmediato justificación detallada de su necesidad y uso previsto.

5. **Transparencia y Gobernanza de IA.** Se promueve la transparencia en los algoritmos de IA utilizados y se establece un sistema de gobernanza robusto. Este sistema incluye auditorías y revisiones periódicas para verificar el cumplimiento de esta política, la efectividad de los controles de seguridad y el correcto uso de las herramientas.

    - **Gestión de Accesos:** La asignación de permisos se basa en el principio del mínimo privilegio. Los derechos de acceso son revisados periódicamente y revocados cuando ya no son necesarios.

    - **Evaluación de Riesgos:** El Director de TIC en conjunto con el auxiliar de seguridad de información y Product Owner analiza el impacto en la seguridad de la información y los riesgos asociados a la privacidad. Estos quedan plasmados en la matriz de riesgos y oportunidades de ISO/IEC 27001:2022

    - **Acciones Correctivas:** Cualquier hallazgo de las auditorías se documentará y dará lugar a la implementación de acciones correctivas para resolver las causas raíz de los problemas detectados y reforzar los controles.

6. **Respuesta Rápida a Incidentes.** Se establece un protocolo de respuesta rápida para actuar de forma eficiente ante cualquier evento y/o incidente de seguridad derivado del uso de IA, como la suplantación de identidad o los deepfakes. Este protocolo se integra con el Sistema de Gestión de Incidentes y la Mesa de Ayuda.

    - **Reporte Inmediato:** Cualquier usuario que detecte un incidente de seguridad (ej. acceso no autorizado, filtración de datos) debe reportarlo inmediatamente a través de la Mesa de Ayuda y/o al auxiliar de seguridad de la información.

- **Clasificación:** El agente de la mesa de ayuda recibe el ticket y lo marca como un "Incidente de Seguridad" de alta prioridad, escalándolo al Comité de Seguridad de la Información.

- **Documentación, análisis y contención:** El Comité de Seguridad de la Información evaluará la gravedad del evento e incidente de seguridad, coordinará la investigación y definirá las acciones de contención inmediatas, como la revocación de accesos o el bloqueo de una cuenta.
  El equipo de TIC documentará el evento y/o incidente, analizará sus causas y registrará todas las acciones tomadas para su gestión.

- **Resolución y Cierre:** Se implementan las medidas correctivas para resolver el evento y/o incidente y prevenir su recurrencia. Esto incluye refuerzos técnicos, refuerzo de controles o capacitación adicional.

- **Actualización documental:** Si el análisis lo requiere, se actualizarán los procedimientos para fortalecer la capacidad de respuesta de Ingeomega.

4. **Responsabilidades**

- **Director de TI:** Es responsable de aprobar la adquisición de licencias de IA, liderar la actualización de esta política y supervisar el cumplimiento general de sus lineamientos.
- **Product Owner:** Gestiona la asignación y configuración de cuentas de IA, asegurando la implementación de controles de seguridad como la autenticación de doble factor (2FA).
  Asegurar la concientización sobre las políticas de uso se continuar llevando un registro de los usuarios capacitados.
  Garantizar un inventario actualizado de todas las licencias de IA aprobadas, los usuarios asignados y los permisos configurados.
- **Usuarios:** Son responsables de cumplir con esta política, proteger sus credenciales de acceso, utilizar las herramientas de IA de forma ética y reportar cualquier evento y/o incidente de seguridad.
- **Auxiliar Seguridad de Información:** Supervisa y audita la aplicación de esta política y los controles asociados para garantizar la seguridad de la información.
  Realizar auditorías sobre el uso de las herramientas de IA para verificar el cumplimiento de las políticas, incluye la revisión de configuraciones de seguridad, activación obligatoria de la Autenticación de Doble Factor (2FA) y derechos de acceso
- **Comité Seguridad de Información:** Analiza y trata los eventos e incidentes y evaluará los riesgos emergentes del uso de la IA en Ingeomega.

5. **Sanciones** El incumplimiento de esta política dará lugar a sanciones que pueden incluir la suspensión temporal o revocación permanente de licencias, así como otras medidas disciplinarias conforme al reglamento interno de trabajo.

A.5.34 Política privacidad y protección de información personal.

Establecer los lineamientos para la protección de la Información de Identificación Personal dentro de Ingeomega S.A.S. garantizando el cumplimiento de los requisitos legales, normativos y contractuales aplicables.

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que tengan acceso, procesen o almacenen información personal en el marco de las operaciones de Ingeomega S.A.S.

La política de privacidad y protección de la información personal está publicada en la página de Ingeomega: https://ingeomega.com.co/politica-de-privacidad/

A.7.7 Política de escritorio y pantalla limpios

Con el fin de reducir los riesgos de acceso indebido, pérdida o daño en la información se establecen los siguientes procedimientos:

A. Almacenar bajo llave los documentos físicos cuando no estén siendo utilizados.
B. Bloquear la sesión de los computadores cuando no se estén usando. Automáticamente se tiene configurado que el equipo se bloquea después de 5 minutos de inactividad, pero es responsabilidad del usuario bloquear el equipo cuando se ausenta.
C. Retirar inmediatamente los documentos enviados para imprimir. De los sitios de impresión
D. La pantalla de bienvenida de los sistemas operativos de los computadores no debe tener accesos a contenido directo a ninguna información.

A.8.1. Política de dispositivo final del usuario.

Ingeomega S.A.S. reconoce la importancia de proteger la información almacenada, procesada o accesible a través de dispositivos finales del usuario, incluidos teléfonos móviles, laptops y estaciones de trabajo. La organización establece directrices específicas para garantizar la seguridad de estos dispositivos, minimizando riesgos como la pérdida, acceso no autorizado o alteración de la información.

- Los dispositivos asignados estarán sujetos a protección contra malware, y configuraciones que aseguren la seguridad de la información.

- Queda prohibido almacenar información secreta o clasificada de Ingeomega S.A.S. en dispositivos no corporativos o en medios locales.
- Se implementan medidas como la desactivación remota de acceso en caso de pérdida o robo, así como el análisis periódico del comportamiento del usuario.

- Las conexiones inalámbricas deberán seguir procedimientos que garanticen su seguridad, utilizando configuraciones adecuadas y desactivando protocolos vulnerables.

- **Responsabilidades del usuario:**
  Los usuarios asignados deben:

A. Asegurar la protección física de los dispositivos mediante controles como el uso de contraseñas
B. Respetar la normativa sobre el tratamiento y protección de datos personales
C. Utilizar dispositivos corporativos exclusivamente para fines laborales.

Lo siguiente, apoya la política de dispositivo final del usuario:

Gestión de los activos de información y equipos de procesamiento de la información**.** **SP-5-509-**	Lineamientos para el control de inventario, asignación y reintegro de dispositivos
Ciclo de vida de la información digital **SI-5-516-**	Controles de seguridad definidos en el modelo de seguridad de la información.

Procedimiento control de acceso a la información **SP-5-503-**	Lineamientos respecto a las solicitudes de alta y baja para los accesos a la información almacenada o transportada.
Manual de almacenamiento en medios magnéticos **SP-5-505-**	Condiciones que garanticen la protección de la información generada y almacenada en medios magnéticos

- **Política de uso del celular en Ingeomega S.A.S.**

La organización reconoce la importancia de la comunicación y la conectividad en los procesos, productos y/o servicios realizados por sus empleados, contratistas o terceros, así mismo, en búsqueda de minimizar los riesgos dadas las vulnerabilidades en la conectividad móvil se hace necesario establecer conciencia con criterios básicos de orientación en el uso de estos dispositivos:

A. Para el uso del celular se debe respetar las normas y recomendaciones del plan estratégico de seguridad vial y SST (Seguridad y salud en el trabajo)
B. El consumo de los servicios móviles debe tener como prioridad la utilización para fines estrictamente laborales.
C. No está permitido el almacenamiento de información de Ingeomega S.A.S. en los dispositivos móviles.
D. No se permite conexión de dispositivos móviles a ninguna red de datos a la que están conectados activos de información y aplicaciones críticas.

A.8.12 Política de prevención de fuga/pérdida de datos (DLP)

- **Objetivo**

Establecer lineamientos para prevenir la fuga o pérdida de información sensible, confidencial o secreta a través del uso del correo electrónico corporativo en Office 365, garantizando la protección de los activos de información.

- **Lineamiento**

Todos los usuarios deben clasificar manualmente los documentos y correos electrónicos según su nivel de sensibilidad: público, interno, clasificado, secreto o personal. Esta clasificación activa automáticamente las políticas de protección y monitoreo configuradas en Microsoft Purview.

El envío de información etiquetada como clasificada o secreta a destinatarios externos está restringido. Solo podrá realizarse mediante cifrado y con la debida autorización. Además, todos los archivos adjuntos enviados por correo electrónico serán analizados por Microsoft Defender for Office 365 antes de ser entregados al destinatario, con el fin de detectar contenido malicioso o no autorizado.

Las políticas de DLP están diseñadas para generar alertas automáticas ante intentos de envío indebido de información sensible. Estas alertas serán revisadas cada trimestre por el equipo de seguridad, quien tomará las acciones correctivas correspondientes. En caso de que se detecten falsos positivos, como la identificación errónea de datos personales o financieros, el incidente será escalado a Microsoft para su análisis y ajuste.

Complementariamente, se mantiene activa la configuración de DKIM y DMARC para garantizar la autenticidad de los correos salientes y prevenir suplantaciones de identidad.

Los usuarios son responsables de clasificar correctamente la información y cumplir con las restricciones establecidas. El área de TI se encargará de configurar y mantener las políticas de seguridad, mientras que el equipo de Seguridad de la Información auditará su cumplimiento y gestionará los incidentes.

A.8.13 Política de copias de seguridad.

La política de copias de seguridad de la información en Ingeomega S.A.S. establece los lineamientos para la gestión de copias de seguridad, asegurando la disponibilidad e integridad de la información crítica y minimizando riesgos asociados con la pérdida de datos, fallos de sistemas o incidentes de seguridad de la información.

Esta política se aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI) de Ingeomega S.A.S., abarcando todas las tecnologías de la información y de la comunicación utilizadas dentro del alcance del SGSI. Esto incluye todos los sistemas de información, bases de datos y archivos críticos de la organización. Además, se aplica a todos los empleados, contratistas y terceros que gestionen activos de información en Ingeomega S.A.S., así como a la infraestructura tecnológica utilizada para el almacenamiento y procesamiento de información.

La Dirección TIC's es responsable de la implementación, supervisión y auditoría de las copias de seguridad, mientras que los usuarios finales son responsables de almacenar información en las ubicaciones designadas para su respaldo. El proveedor de infraestructura es responsable de garantizar la disponibilidad y seguridad de los servicios de almacenamiento en la nube, si se utilizan servicios externos.

Se debe garantizar la generación continua de copias de respaldo y el almacenamiento seguro de la información crítica, proporcionando los recursos para medios de respaldo adecuados y estableciendo los procedimientos y mecanismos para la realización de estas actividades de manera efectiva, con el fin de asegurar que toda la información esencial de la entidad pueda ser restaurada en caso de ser necesario.
El almacenamiento de la información se debe realizar de manera interna y externa, de acuerdo con su clasificación y con previa validación del Líder de Seguridad de la Información.
Las copias de respaldo se deben almacenar en un sitio lejano con protección física, lógica y ambiental, a una distancia suficiente para escapar a cualquier daño causado por desastres. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados y, en lo posible, estar certificados en la gestión de seguridad de la información.
Se recomienda usar otra locación externa o ver la viabilidad de uso de empresas en el mercado que se dedican a esto de manera segura y confiable.
Los procedimientos de restauración para los medios de respaldo se verificarán de acuerdo con el cronograma de comprobación de recursos para garantizar la disponibilidad de la información en caso de contingencia o desastre.
Las copias de seguridad de computadores y equipos portátiles son obligación de cada responsable de dicho equipo y se deben realizar de acuerdo con el software suministrado por la organización.
Se deben hacer copias de respaldo de la información y del software con una periodicidad establecida en el manual de copias de seguridad para garantizar la integridad y disponibilidad. Las especificaciones detalladas técnicamente para la realización de las copias de seguridad se encuentran en el SP-5-511-Manual Copia de seguridad, el cual debe ser actualizado de acuerdo con cambios en la matriz de activos que lo impacten, y en los cambios del negocio que a su vez impacten el plan de continuidad.

A.8.24 Política de uso de criptografía

En Ingeomega se aplican mecanismo y herramientas para la encriptación y el cifrado seguro de algunos datos con el fin de garantizar la disponibilidad, confidencialidad e integridad de la información clasificada y secreta, como en los siguientes casos

- ✓ Protección de claves de acceso a sistemas, datos y servicios.
- ✓ Transmisión de información clasificada como sensible.
- ✓ Resguardo de información, cuando así surja de la evaluación de riesgos

En Ingeomega se hace énfasis en la protección de la información catalogada como secreta y clasificada aplicando técnicas de encriptación o de custodia al momento de almacenarse o transmitirse por cualquier medio. Para dar cumplimiento al tratamiento definido para los activos de información, todos los miembros de la organización deben cumplir, las siguientes directrices según les aplique:

1. En sistemas de información y aplicaciones que presten servicios web, se aplican algoritmos de cifrado simétricos AES-256 o asimétrico RSA-4096.
2. Ningún miembro de la organización está autorizado para encriptar información enviada por medio de correo electrónico.
3. En el acceso a activos y servicios de red se aplican herramientas de cifrado WPA3 y TLS 1.2 o superior
4. Todos los miembros de la organización deben almacenar la información clasificada y secreta en la nube, no se permite realizar almacenamiento de esta en discos duros o equipos que se transporten por fuera del edificio.
5. Los controles de acceso suministrados por las entidades financieras y transaccionales como tokens estarán bajo la custodia del Gerente financiero en una caja fuerte, sólo el Gerente general y Gerente financiera tendrán acceso a esta.
6. Para la solicitud, gestión y recuperación de acceso a componentes corporativos mediante claves de acceso, es requisito que se realice a través de un ticket de soporte.
7. Todos los accesos a información crítica deben utilizar autenticación de múltiples factores (MFA/2FA).

- **Política de gestión de llaves:**

Esta política describe los requisitos para proteger las llaves/claves de cifrado que se encuentran bajo el control de los usuarios finales en nuestra organización. A través de esta se promueve y garantiza su uso correcto para conducir al compromiso y divulgación que las llaves/claves privadas se utilicen para proteger los datos sensibles y por tanto el compromiso de los datos.

Nota: Cuando nos refiramos a tecnología PKI utilizaremos la palabra “Llave” y cuando nos refiramos a una contraseña para cifrado simétrico utilizaremos la palabra “Clave” y cuando no refiramos a las dos tecnologías usaremos llaves/claves

- **Objetivo**

Esta política describe los requisitos para proteger las llaves/claves de cifrado que se encuentran bajo el control de los usuarios finales. Estos requisitos están diseñados para evitar la divulgación no autorizada y su posible uso fraudulento posterior. Los métodos de protección previstos incluirán controles operacionales y técnicos, tales como procedimientos de copias de seguridad, cifrado bajo una llave/claves distintas y el uso de hardware reforzado en seguridad

- **Alcance**

Esta política aplica a cualquiera llave/claves de cifrado listada a continuación y a cualquier persona responsable de alguna de estas llaves/claves de cifrado. Las llaves/claves de cifrado cubiertas por esta política son:

A. Llaves/claves de cifrado emitidas por la empresa
B. Llaves/claves de cifrado utilizadas para negocios de la empresa
C. Llaves/claves de cifrado utilizadas para proteger datos propiedad de la empresa

Las llaves públicas contenidas en los certificados digitales están explícitamente exentas de esta política 4. Política Todas las llaves/claves de cifrado cubiertas por esta política deben ser protegidas para evitar su divulgación no autorizada y su posible uso fraudulento posterior.