GRIJALVA TECNOLOGÍA

SOP-EDM-01-M02
MANUAL DE POLÍTICAS DE INTELIGENCIA ARTIFICIAL

Dirección de Operaciones

Tel.
(55) 53394720
(55) 53394730

Mail
gobierno@solteg.com.mx

RFC
STG-140703-HV0

Dirección
Londres 87, Col. de Carmen, Alc. Coyoacán,
C.P. 04100, Ciudad de México

GRIJALVA TECNOLOGÍA

Tabla de contenido

GRIJALVA TECNOLOGÍA

GRIJALVA TECNOLOGÍA

GRIJALVA TECNOLOGÍA

GRIJALVA TECNOLOGÍA

GRIJALVA TECNOLOGÍA

1. Introducción

El presente Manual del Sistema de Gestión de Inteligencia Artificial (SGIA) establece el conjunto integral de lineamientos, políticas, directrices y criterios operativos que orientan el diseño, desarrollo, despliegue, operación, evaluación, mantenimiento y retiro de los sistemas de Inteligencia Artificial dentro de SOLTEG. Su propósito es garantizar que el uso de la IA se lleve a cabo bajo principios de ética, responsabilidad, seguridad, transparencia, equidad y trazabilidad, en plena conformidad con los requisitos establecidos por la norma ISO/IEC 42001:2023 y con la legislación aplicable.

Este manual constituye el marco rector para gestionar de manera sistemática los riesgos asociados al ciclo de vida del sistema de IA de SOLTEG, promover la mejora continua, asegurar la calidad de los datos y modelos, y fortalecer la confianza de usuarios internos, externos y partes interesadas. Asimismo, define con claridad las responsabilidades institucionales, los roles operativos, las prácticas técnicas, los controles de supervisión humana y los mecanismos de monitoreo necesarios para que los sistemas de IA contribuyan de manera segura, eficaz y alineada con los valores corporativos al logro de los objetivos estratégicos de SOLTEG.

2. Objetivo

El objetivo de este manual es establecer una guía documental clara, estructurada y accesible que consolide las políticas, criterios, responsabilidades y lineamientos operativos que integran el Sistema de Gestión de Inteligencia Artificial (SGIA). Su función principal es servir como documento rector que facilite la aplicación uniforme de los procesos, prácticas y controles definidos, garantizando que todas las áreas de SOLTEG comprendan sus responsabilidades y actúen conforme a los principios del SGIA.

Asimismo, este manual tiene como propósito estandarizar procedimientos, fortalecer la trazabilidad de las actividades relacionadas con la gestión de la IA y proporcionar la evidencia documental necesaria. Con ello se asegura la coherencia, transparencia y alineación del SGIA con los requisitos de la norma ISO/IEC 42001:2023 y con la normativa vigente aplicable.

GRIJALVA TECNOLOGÍA

3. Alcance

El alcance del SGIA comprende a todas las partes interesadas de SOLTEG, incluyendo a las áreas que participan en el diseño, desarrollo, operación, supervisión, control, gestión de riesgos y aseguramiento de los sistemas de Inteligencia Artificial. El SGIA aplica a todas las actividades relacionadas con el ciclo de vida de los sistemas de IA, desde la planeación y definición de requisitos hasta el monitoreo, mantenimiento y retiro.

El alcance incluye:

- Todos los sistemas, aplicaciones, herramientas y procesos que integren componentes de IA desarrollados internamente o adquiridos a terceros.
- Todo el personal involucrado en actividades de datos, desarrollo, infraestructura, operación, seguridad, cumplimiento, auditoría y supervisión humana significativa.
- La gestión de riesgos, controles, métricas, documentación, incidentes y cumplimiento regulatorio relacionados con IA.
- Los procesos de soporte asociados: gestión de datos, ciberseguridad, recursos humanos, compras, jurídico, aseguramiento de procesos y control interno.

Quedan excluidas únicamente las actividades, sistemas o herramientas tecnológicas que no incorporen ningún componente de IA ni influyan en sistemas que sí la contengan.

4. Aplicabilidad

El SGIA es aplicable a todo el personal, áreas, procesos, tecnologías, proveedores y sistemas que formen parte del ciclo de vida de los sistemas de Inteligencia Artificial dentro de SOLTEG. La aplicabilidad incluye tanto a quienes desarrollan, operan, supervisan o mantienen sistemas de IA, como a quienes participan en actividades de apoyo que influyen en su funcionamiento seguro y conforme a los requisitos normativos.

Esta aplicabilidad abarca:

- Todas las unidades organizacionales con interacción directa o indirecta con sistemas de IA.
- Todo el personal que desempeña funciones directivas, operativas, técnicas, jurídicas, de auditoría, de aseguramiento y de control interno.
- Todos los sistemas de IA propios o adquiridos, así como sus componentes de datos, algoritmos, infraestructura y procesos asociados.
- Proveedores y terceros que intervengan en la provisión de datos, desarrollo, mantenimiento, análisis, consultoría o servicios de IA.

El SGIA es obligatorio para todos los colaboradores incluidos en su alcance, quienes deberán

cumplir las políticas, procedimientos, lineamientos y controles establecidos. Cualquier excepción debe estar documentada, justificada y aprobada por el Líder del SGIA.

5. Términos y definiciones

Inteligencia Artificial (IA): Sistema basado en técnicas computacionales capaces de realizar tareas que requieren razonamiento o aprendizaje humano.

Sistema de IA: Aplicación que utiliza modelos, datos y algoritmos para generar decisiones, predicciones, clasificaciones o recomendaciones.

Modelo de IA: Implementación matemática o estadística entrenada con datos para producir un resultado específico.

Entrenamiento de modelo: Proceso mediante el cual un modelo ajusta parámetros a partir de datos para mejorar su desempeño.

Datos de entrenamiento / validación / prueba: Conjuntos de datos utilizados para entrenar, ajustar y evaluar un modelo de IA.

Ciclo de vida del sistema de IA: Etapas del sistema desde su diseño, desarrollo y entrenamiento, hasta operación, monitoreo, mantenimiento y retiro.

Supervisión humana significativa: Intervención humana con autoridad real para modificar, detener o revertir las decisiones de un sistema de IA.

Sesgo algorítmico: Distorsión en los resultados del sistema causada por errores en datos, modelos o procesos.

Transparencia: Capacidad de entender cómo funciona un sistema de IA y por qué genera un resultado.

Explicabilidad: Claridad proporcionada al usuario o auditor para interpretar los resultados del sistema de IA.

Deriva del modelo (Model Drift): Pérdida de desempeño debida a cambios en datos o condiciones del entorno.

Robustez: Capacidad del sistema de IA de mantener su comportamiento esperado bajo

condiciones adversas.

Riesgo de IA: Posibilidad de impacto negativo ocasionado por resultados o fallas del sistema de IA.

Evaluación de Impacto de IA (IA-PIA): Proceso sistemático para identificar riesgos y evaluar efectos no deseados en sistemas de IA.

Trazabilidad de IA: Capacidad de registrar decisiones, versiones, datos, configuraciones y acciones dentro del ciclo de vida del sistema.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluar si se cumplen criterios de auditoría.

Criterios de auditoría: Conjunto de políticas, requisitos, procedimientos o normas utilizados como referencia para evaluar evidencia.

Evidencia de auditoría: Registros, declaraciones o información verificable utilizada para determinar el cumplimiento.

Hallazgo de auditoría: Resultado de la evaluación de evidencias frente a los criterios de auditoría.

No conformidad: Incumplimiento de un requisito establecido por SOLTEG o por una norma.

Acción correctiva: Acción para eliminar la causa raíz de una no conformidad y prevenir su recurrencia.

Competencia (en auditoría): Aptitud demostrada para aplicar conocimientos y habilidades.

Programa de auditoría: Conjunto de una o más auditorías planificadas para un periodo específico.

Equipo auditor: Grupo de personas que lleva a cabo una auditoría, incluyendo al auditor líder y auditores técnicos.

Auditor líder: Persona responsable de planear, conducir y cerrar la auditoría.

Objeto de auditoría: Proceso, sistema o área que se evalúa durante la auditoría.

Parte interesada: Individuo o grupo afectado por los resultados del SGIA o por las auditorías.

6. Política General y de Gobernanza del Sistema de Gestión de IA (SGIA)

SOLTEG establece y mantiene el Sistema de Gestión de Inteligencia Artificial (SGIA) con el propósito de garantizar que el diseño, desarrollo, adquisición, implementación, operación, mantenimiento y mejora de los sistemas de inteligencia artificial se realice de manera ética, responsable, segura, fiable, transparente y conforme a las obligaciones legales, regulatorias, contractuales y normativas aplicables, incluyendo los requisitos establecidos en la ISO/IEC 42001:2023.

SOLTEC se compromete a que todos los sistemas de IA bajo su control cumplan los siguientes principios:

- Gestión del riesgo y seguridad: Identificar, evaluar, prevenir, mitigar y monitorear los riesgos asociados con el ciclo de vida de los sistemas de IA, considerando impactos en personas, procesos, activos, infraestructura y entorno. Establecer controles adecuados a la clasificación del sistema, su nivel de riesgo, criticidad, impacto y casos de uso.

- Protección de datos y privacidad: Garantizar el tratamiento adecuado, seguro y lícito de los datos personales, sensibles y confidenciales utilizados por los sistemas de IA. Así como aplicar medidas de privacidad desde el diseño y por defecto (Privacy by Design & Default).

- Transparencia, explicabilidad y trazabilidad: Asegurar la existencia de mecanismos que permitan comprender el funcionamiento, decisiones y resultados de los sistemas de IA, en la medida compatible con la tecnología, el riesgo y el contexto. Mantener trazabilidad del ciclo de vida de modelos, datos, versiones, decisiones automatizadas y registros relevantes.

- Supervisión humana significativa: Establecer roles, responsabilidades y competencias para garantizar una supervisión humana apropiada, así como evitar dependencias excesivas de la automatización y preservar la capacidad de intervención humana cuando sea necesario.

- Ética, equidad y confiabilidad: Promover el uso responsable, equitativo y no

discriminatorio de los sistemas de IA. Prevenir sesgos indebidos, uso indebido, efectos adversos o resultados no deseados derivados de los modelos o datos utilizados.

- Gobernanza, responsabilidad y cumplimiento normativo: Cumplir con las disposiciones legales y regulatorias nacionales e internacionales aplicables. Asegurar que los sistemas de IA respeten los principios de gobernanza, integridad, responsabilidad y rendición de cuentas.

- Gestión de proveedores y partes externas: Evaluar y controlar riesgos asociados con servicios de IA, proveedores, modelos externos, datasets de terceros y componentes adquiridos o utilizados externamente.

- Mejora continua: Evaluar de forma periódica la eficacia del SGIA, incluyendo auditorías internas, revisiones por la dirección, análisis de desempeño, monitoreo de incidentes y retroalimentación de usuarios. Mejorar de manera continua los procesos, modelos, controles y mecanismos de gobernanza relacionados con IA.

Compromiso de la Alta Dirección de SOLTEG

La alta dirección se compromete a:

- Proveer los recursos humanos, tecnológicos, financieros y de infraestructura necesarios para la operación eficaz del SGIA.

- Asegurar la competencia, capacitación y concientización del personal involucrado en sistemas de IA.

- Promover una cultura de responsabilidad, ética y uso seguro de la IA.

- Garantizar la comunicación, consulta y difusión de esta política dentro de toda SOLTEG y a las partes interesadas pertinentes.

- Supervisar el desempeño del SGIA y asegurar su alineación con los objetivos estratégicos de SOLTEG.

6.1 Objetivo

Establecer el compromiso institucional para desarrollar, utilizar, operar y mejorar los

sistemas de Inteligencia Artificial de manera ética, responsable, segura, transparente y conforme a las leyes aplicables, orientado a garantizar que cualquier proceso relacionado con IA en SOLTEG se efectúe en apego a los principios de gobernanza., gestión de riesgos, protección de datos, supervisión humana significativa y mejora continua.

6.2 Alcance

Esta política aplica a todas las actividades, procesos, proyectos, sistemas y servicios que involucren el desarrollo, uso, adquisición, evaluación, operación, mantenimiento o retiro de tecnologías de Inteligencia Artificial de SOLTEG, incluyendo a todas las áreas y personal que participe directa o indirectamente en iniciativas de IA, así como a proveedores, consultores y terceros que intervengan en su desarrollo o soporte; abarcando también los datos, modelos, algoritmos, herramientas y plataformas utilizadas en cualquier etapa del ciclo de vida de los sistemas de IA, sin importar su nivel de riesgo, complejidad o propósito.

6.3 Responsabilidades

6.3.1. Las partes interesadas internas del Sistema de Gestión de Inteligencia Artificial (SGIA) son responsables de implementar la Política de Gobernanza y Gestión de IA dentro de sus áreas de responsabilidad, asegurando su correcta aplicación en todas las actividades que involucren sistemas, procesos o decisiones habilitadas por IA.

6.3.2. Las partes interesadas del SGIA son responsables de cumplir con la Política de Gobernanza y Gestión de IA, abstenerse de realizar prácticas que vulneren sus lineamientos y notificar oportunamente cualquier incumplimiento, desviación o riesgo identificado que pueda comprometer la integridad del sistema de gestión.

6.3.3. El Senior Management Team es responsable de elaborar, revisar, actualizar y aprobar la Política de Gobernanza y Gestión de IA; asimismo, garantizar los recursos necesarios para su implementación y mejora continua. Las partes interesadas podrán proponer mejoras cuando lo consideren pertinente. Así mismo “SOLTEG establece un único Comité del Sistema de Gestión, el cual funge también como Comité de Riegos y control del SGIA. Este comité multidisciplinario coordina la revisión del desempeño, la supervisión humana significativa, la gestión de riesgos, el análisis ético de los sistemas de IA y la toma de decisiones relacionadas con la operación, mejora y cumplimiento del SGIA conforme a ISO/IEC 42001.”

6.3.4. El Líder de Órgano Interno de Control es responsable de definir el modelo de gobernanza de IA, asegurar su implementación, coordinar la gestión de riesgos asociados a los sistemas de IA y evaluar la correcta aplicación de la metodología de identificación, análisis, evaluación y tratamiento de riesgos.

GRIJALVA TECNOLOGÍA

6.3.5. El Auditor Interno es responsable de monitorear y dar seguimiento al cumplimiento de la presente política, verificar que se mantenga actualizada y asegurar su adecuada difusión dentro de SOLTEG, conforme a los requisitos de auditoría interna establecidos.

6.3.6. El Gerente de Recursos Humanos es responsable de comunicar al personal de nuevo ingreso las obligaciones derivadas de esta política, así como difundir de manera oportuna cualquier modificación, actualización o nuevo lineamiento aprobado por el SGIA.

6.3.7. El Director de Operaciones es responsable de notificar a las partes interesadas externas del SGIA sobre las obligaciones relacionadas con esta política, así como comunicar cualquier cambio o actualización que pudiera impactar su cumplimiento.

6.3.8. El Director de Operaciones es responsable de establecer e implementar los mecanismos de control necesarios para la operación segura, ética y conforme a los principios de gobernanza de todos los sistemas, modelos, datasets, herramientas y recursos tecnológicos utilizados en soluciones de IA.

6.3.9. El Auditor Interno es responsable de diseñar, programar y ejecutar auditorías internas del Sistema de Gestión de IA que verifiquen el cumplimiento de la presente política y del marco de control establecido por SOLTEG.

6.3.10. Los Líderes de Desarrollo de IA, Operaciones y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA deben asegurarse de que todos los procedimientos operativos relacionados con el ciclo de vida de los sistemas de IA —incluyendo diseño, entrenamiento, validación, despliegue, monitoreo y retiro— se ejecuten correctamente y en alineación con las políticas, estándares y controles del SGIA.

6.3.11. El Líder de Órgano Interno de Control es responsable de realizar trimestralmente la identificación y evaluación de vulnerabilidades, riesgos, impactos y amenazas relacionados con los sistemas de IA, conforme a la metodología de gestión de riesgos establecida por SOLTEG.

6.3.12 La presente política deberá ser revisada de manera anual y/o cuando surjan actualizaciones a la misma, estos cambio y/o modificaciones y actualizaciones deben ser aprobados por el SMT y comunicados por el Líder de riesgos y control del SGIA.

GRIJALVA TECNOLOGÍA

6.3.13 El periodo de retención de la información es de por lo menos 5 años, y será definido por el dueño de la información para su posterior destrucción y/o depuración en los sistemas.

6.4 Generalidades

6.4.1. SOLTEG se compromete a desarrollar, operar y mejorar sistemas de inteligencia artificial de manera responsable, ética, segura, transparente y conforme a los requisitos legales y normativos aplicables.

6.4.2. SOLTEG asegura:

- Prevención y mitigación de riesgos asociados al uso de IA.
- Protección de datos personales y sensibles.
- Transparencia y explicabilidad de los sistemas de IA.
- Supervisión humana significativa.
- Mejora continua de procesos, modelos y controles.
- Cumplimiento con estándares internacionales, incluyendo ISO/IEC 42001.

6.4.3. SOLTEG aplicará un enfoque sistemático de gestión de riesgos de IA para identificar, evaluar, tratar y monitorear riesgos en todas las etapas del ciclo de vida de los sistemas de inteligencia artificial.

6.4.4. El diseño, desarrollo, implementación y uso de IA deberán alinearse con principios éticos que garanticen justicia, no discriminación, responsabilidad, seguridad y respeto a los derechos humanos.

6.4.5. Los datos utilizados para el entrenamiento, validación, prueba y operación de los sistemas de IA deberán cumplir con los estándares de calidad, integridad, trazabilidad y gobernanza del dato establecidos por SOLTEG. Además, dichos datos no podrán ser datos reales o verídicos de personas o clientes, sino datos de prueba o datos sintéticos diseñados exclusivamente para estos fines.

6.4.6. Todos los sistemas de IA estarán sujetos a controles y medidas de seguridad de la información para prevenir accesos no autorizados, daños, manipulaciones o ataques adversariales.

6.4.7. Cualquier tratamiento de datos personales dentro de sistemas de IA deberá realizarse conforme a la legislación aplicable, principios de privacidad y mecanismos de protección reforzada para datos sensibles.

6.4.8. Los sistemas de IA deberán contar con supervisión humana significativa, capaz de intervenir, detener o corregir decisiones automatizadas cuando exista riesgo para personas, procesos o activos.

6.4.9. Los sistemas de IA deberán ser transparentes y explicables, proporcionando la claridad necesaria sobre su funcionamiento, criterios de decisión y limitaciones.

6.4.10. Todo modelo de IA deberá ser validado, verificado y monitoreado continuamente para asegurar su desempeño, robustez, ausencia de sesgos no deseados y cumplimiento de los requisitos del SGIA.

6.4.11. Los incidentes relacionados con sistemas de IA deberán registrarse, analizarse y gestionarse bajo un proceso formal que asegure acciones correctivas y la mejora del SGIA.

6.4.12. La actualización, versionamiento y retiro de modelos de IA deberán seguir procedimientos formales que garanticen control, trazabilidad y mitigación de riesgos asociados.

6.4.13. El personal involucrado en el ciclo de vida de los sistemas de IA deberá contar con las competencias, conocimientos y formación requerida para operar y supervisar IA de manera responsable.

6.4.14. Los proveedores y terceros que suministren datos, modelos, plataformas o servicios relacionados con IA deberán cumplir con los lineamientos del SGIA y requisitos contractuales establecidos por SOLTEG.

6.4.15. El SGIA estará sujeto a auditorías internas periódicas que verifiquen su funcionamiento, eficacia, conformidad y oportunidad de implementación.

6.4.16. Los usuarios internos y externos afectados por decisiones automatizadas tendrán derecho a solicitar revisión humana, aclaraciones o impugnación cuando las decisiones de IA tengan impacto significativo.

6.4.17. La alta dirección asegura los recursos necesarios y la comunicación adecuada del SGIA en SOLTEG.

GRIJALVA TECNOLOGÍA

7. Política de Uso Aceptable de IA Generativa

SOLTEG reconoce que el uso de herramientas de Inteligencia Artificial Generativa (IAG) —incluyendo modelos de texto, imagen, video, código y audio— implica riesgos específicos relacionados con la seguridad de la información, privacidad, propiedad intelectual, sesgos, exactitud y cumplimiento regulatorio. La presente política establece los lineamientos para asegurar un uso responsable, seguro, ético y alineado a los objetivos y principios del Sistema de Gestión de Inteligencia Artificial (SGIA), estableciendo reglas claras sobre su utilización, límites operativos, prohibiciones, controles y salvaguardas necesarias para su adecuada adopción dentro de SOLTEG.

7.1 Objetivo

Establecer las directrices, límites, responsabilidades y controles necesarios para garantizar que el uso de herramientas de IA Generativa por parte del personal y terceros se realice de manera segura, ética, conforme a los principios del SGIA, evitando riesgos relacionados con divulgación indebida de información, generación de contenido sesgado o inexacto, vulneración de derechos de autor, exposición de datos sensibles o utilización indebida de los sistemas.

7.2 Alcance

Esta política aplica a todo el personal, contratistas, proveedores, terceros autorizados y cualquier parte interesada interna o externa que utilice herramientas de IA Generativa en actividades laborales, académicas o de soporte relacionadas con SOLTEG, abarcando el uso de plataformas públicas, privadas, APIs, modelos locales, asistentes virtuales y cualquier solución de creación automática de contenido generativo utilizada en procesos operativos, administrativos, técnicos o estratégicos.

7.3 Responsabilidad

7.3.1 Líder de Órgano Interno de Control

Establecer los lineamientos de uso aceptable de IA Generativa, evaluar los riesgos asociados a su adopción, validar las herramientas autorizadas, coordinar la implementación de controles y supervisar el cumplimiento de esta política.

7.3.2 Líderes de Desarrollo de IA, Infraestructura y seguridad de IA y Líder de Operación y soporte de Sistemas de IA

Definir las plataformas autorizadas, aplicar restricciones técnicas, asegurar la protección de datos, prevenir fugas de información y habilitar mecanismos de monitoreo para garantizar el uso seguro de IA Generativa.

7.3.3 Propietarios de Procesos

Identificar los casos de uso permitidos y prohibidos dentro de sus áreas, asegurar que el personal reciba capacitación adecuada y verificar que el contenido generado cumpla con los estándares de calidad, ética y precisión requeridos.

7.3.4 Usuarios

Hacer uso de herramientas de IA Generativa únicamente bajo los lineamientos establecidos, evitar el ingreso de datos sensibles, confidenciales o restringidos y reportar incidentes, resultados irregulares o uso indebido.

7.3.5 Proveedores y Terceros

Cumplir con los lineamientos del SGIA, garantizar que sus herramientas o integraciones de IA Generativa incluyan mecanismos de privacidad, seguridad y transparencia, y proporcionar documentación correspondiente.

7.4 Generalidades

7.4.1 Queda estrictamente prohibido ingresar datos personales, sensibles, confidenciales o estratégicos a herramientas de IA pública sin autorización explícita.

7.4.2 El contenido generado deberá ser revisado, validado y verificado por un humano competente antes de su uso en decisiones, reportes oficiales o entregables críticos.

7.4.3 Se permitirá el uso de IA Generativa únicamente en herramientas autorizadas por el SGIA y el área de Operaciones (TI).

7.4.4 Los sistemas de IA utilizados deberán documentar su propósito, alcance y restricciones, así como sus riesgos identificados.

7.4.5 Queda prohibido utilizar IA Generativa para crear contenido engañoso, manipulador, discriminatorio o que afecte la reputación de SOLTEG.

7.4.6 Toda información generada o utilizada deberá cumplir con legislación aplicable, incluyendo derechos de autor, privacidad y protección de datos.

7.4.7 El personal deberá participar en capacitaciones obligatorias sobre riesgos y lineamientos de uso seguro de IA Generativa.

7.4.8 Cualquier incidente, error, sesgo detectado o comportamiento inesperado deberá ser reportado inmediatamente conforme al proceso de gestión de incidentes del SGIA.

7.4.9 Esta política será revisada al menos una vez al año o cuando existan cambios relevantes en la tecnología, regulaciones o riesgos asociados.

8. Política de Gestión de Riesgos de IA

8.1 Objetivo

Establecer los principios, criterios y directrices para identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados a los sistemas de Inteligencia Artificial de SOLTEG, asegurando que dichos riesgos se gestionen de manera sistemática, proactiva y alineada con los requisitos de ISO 42001 y con los objetivos estratégicos de SOLTEG.

8.2 Alcance

Esta política aplica a todos los sistemas de IA desarrollados, adquiridos, integrados o utilizados por SOLTEG; a todos los procesos relacionados con el ciclo de vida de los sistemas de IA (diseño, desarrollo, implementación, operación, mantenimiento y retiro); y a todo el personal, proveedores y terceros que participen o influyan en la gestión de riesgos asociados al uso de IA.

8.3 Responsabilidades

8.3.1 El Líder de Órgano Interno de Control es responsable de:

- Supervisar la correcta aplicación del proceso de gestión de riesgos de IA.
- Aprobar los criterios de riesgo y los métodos para su evaluación.
- Presentar los resultados de la gestión de riesgos ante la alta dirección.

8.3.2 Equipos propietarios de los sistemas de IA:

- Identificar y documentar los riesgos propios de cada sistema de IA en todas las fases del ciclo de vida.
- Implementar las acciones de tratamiento definidas.
- Mantener actualizados los registros y la evidencia de la gestión de riesgos.

8.3.3 Equipo de Gobernanza de IA / Comité de IA:

- Revisar y validar los riesgos críticos y su tratamiento.
- Asegurar la alineación entre riesgos, controles y cumplimiento normativo.

8.3.4 Usuarios y Operadores de los sistemas de IA**:**

- Reportar oportunamente incidentes, desviaciones o riesgos emergentes.
- Cumplir con las medidas y controles establecidos para minimizar riesgos.

8.3.5 Proveedores y terceros relacionados:

- Cumplir con los requisitos de gestión de riesgos establecidos por SOLTEG.
- Entregar información completa y verificable sobre los riesgos asociados a las soluciones de IA entregadas.

8.4 Generalidades

8.4.1 SOLTEG implementa un proceso sistemático para identificar, evaluar, priorizar y tratar riesgos asociados al diseño, desarrollo, implementación y operación de sistemas de IA.
Esto incluye:

- Evaluaciones de impacto (IA-PIA).
- Clasificación del sistema de IA (riesgo, impacto, uso).
- Registro y tratamiento de riesgos.
- Monitoreo continuo de riesgos emergentes.

8.4.2 Los sistemas clasificados como alto riesgo deben incluir medidas adicionales de control, trazabilidad y supervisión humana.

8.4.3 SOLTEG adopta un enfoque de gestión de riesgos continua, considerando riesgos técnicos, éticos, legales, operativos, reputacionales y de impacto en personas y procesos.

8.4.4 La evaluación de riesgos se deberá realizar previo al desarrollo o adquisición de cualquier sistema de IA, y actualizarse ante cambios significativos, incidentes o hallazgos de auditoría.

8.4.5 Los riesgos deberán clasificarse con base en su probabilidad, severidad e impacto potencial, utilizando criterios definidos y documentados.

8.4.6 Los controles, medidas de mitigación y aceptaciones de riesgo deberán quedar registrados en la Matriz de Riesgos de IA.

8.4.7 La gestión de riesgos deberá integrarse con la gestión de cambios, la gobernanza de

datos, la seguridad de la información, la protección de derechos fundamentales y con el ciclo de vida de los sistemas de IA.

8.4.8 En caso de riesgos altos o críticos no mitigables, SOLTEG evaluará la suspensión, rediseño o cancelación del sistema de IA.

9. Política de Gestión del Ciclo de Vida de Sistemas de IA

9.1 Objetivo

Establecer los lineamientos para la gestión integral del ciclo de vida de los sistemas de inteligencia artificial, desde su concepción y diseño hasta su despliegue, operación, monitoreo, mejora continua y retiro, asegurando que cada fase sea realizada de manera ética, segura y transparente.

9.2 Alcance

Esta política aplica a todos los sistemas, modelos, algoritmos, datasets, herramientas, componentes tecnológicos, proveedores y procesos relacionados con el ciclo de vida de soluciones basadas en inteligencia artificial desarrolladas, adquiridas, implementadas o utilizadas por SOLTEG. Incluye actividades técnicas, operativas, administrativas y de soporte vinculadas al diseño, entrenamiento, validación, despliegue, mantenimiento, monitoreo, actualización y retiro seguro de sistemas de IA.

9.3 Responsabilidades

9.3.1. Líder de Órgano Interno de Control:

- Establecer y mantener el modelo de gestión del ciclo de vida de IA.
- Aprobar metodologías, plantillas y criterios aplicables a cada fase.
- Asegurar la integración del riesgo, ética, privacidad, seguridad y explicabilidad en cada etapa del ciclo de vida.

9.3.2. Líderes de Desarrollo de IA, Operaciones y Soporte de sistemas de IA e Infraestructura y seguridad de IA:

- Implementar los procesos, controles y buenas prácticas definidos para todas las fases del ciclo de vida.
- Gestionar versiones, trazabilidad, repositorios, documentación técnica, control de cambios y evidencias.
- Garantizar el funcionamiento seguro y conforme a los lineamientos del SGIA.

9.3.3. Auditor Interno:

- Verificar que las actividades del ciclo de vida cumplan con esta política.
- Confirmar la existencia de controles de diseño, validación, pruebas, despliegue y monitoreo continuo.
- Emitir hallazgos, oportunidades de mejora y acciones correctivas.

9.3.4. Dueños de Proceso / Partes Interesadas Internas:

- Identificar requerimientos funcionales, legales, operativos y éticos aplicables al sistema de IA.
- Participar en pruebas, validaciones y revisiones de desempeño.
- Reportar desviaciones, incidentes o fallos detectados durante la operación.

9.3.5. Proveedores y Terceros Tecnológicos:

- Cumplir con los requisitos de diseño, entrega, soporte y mantenimiento definidos por SOLTEG.
- Proporcionar evidencia suficiente de calidad, seguridad, gobernanza y funcionalidad de sus modelos y datos.

9.4 Generalidades

9.4.1 Se deberán aplicar controles en todas las fases del ciclo de vida estandarizado de los sistemas de IA, incluyendo:

- Gobernanza y análisis de viabilidad del caso de uso
- Diseño y definición de requisitos
- Recolección, preparación y gestión de datos
- Desarrollo del modelo
- Validación, verificación y pruebas
- Implementación y despliegue
- Operación, monitoreo y control
- Mantenimiento, reentrenamiento y mejora continua
- Retiro, desmantelamiento o reemplazo

9.4.2. Trazabilidad y documentación obligatoria:
Todas las fases del ciclo de vida deben registrar evidencia verificable, incluyendo datasets utilizados, versiones de modelos, resultados de pruebas, métricas de desempeño, controles aplicados y decisiones clave.

9.4.3. Calidad, seguridad y privacidad por diseño
Todo sistema de IA deberá incorporar, desde su diseño y a lo largo de su ciclo de vida,

mecanismos que garanticen:

- Protección de datos personales
- Mitigación de sesgos y tratamiento justo
- Explicabilidad y transparencia del sistema
- Seguridad técnica y ciberseguridad
- Supervisión y control humano significativo
- Robustez, resiliencia y desempeño confiable

9.4.4. Validación continua:
Los sistemas de IA deben ser evaluados periódicamente para detectar degradación del modelo, sesgos emergentes, variaciones en datos, fallos operativos o desviaciones respecto a los objetivos originales.

9.4.5. Gestión del cambio y de versiones:
Toda actualización de modelos, algoritmos, datasets o infraestructura deberá ser registrada, evaluada, probada y aprobada antes de su implementación.

9.4.6. Retiro seguro del sistema de IA:
Cuando un sistema de IA se considere obsoleto, riesgoso o fuera de operación, deberá retirarse de forma controlada, garantizando la eliminación segura de datos, modelos y accesos, y dejando evidencia formal del cierre.

10. Política de Calidad y Gestión de Datos

10.1 Objetivo

Establecer los principios, lineamientos y controles para asegurar la calidad, integridad, disponibilidad, confiabilidad, seguridad y uso ético de los datos utilizados en el desarrollo, entrenamiento, validación, operación y mantenimiento de los sistemas de inteligencia artificial, garantizando que todos los datasets empleados cumplan con requisitos técnicos, regulatorios, de privacidad, gobernanza y trazabilidad de SOLTEG.

10.2 Alcance

Esta política aplica a todos los datos utilizados por sistemas de IA (estructurados, no estructurados, semiestructurados), datos internos, externos, adquiridos, generados o derivados, todas las fases del ciclo de vida de IA: recolección, preparación, transformación, etiquetado, entrenamiento, validación, pruebas, operación, monitoreo y retiro. Y todo el

personal, áreas, proveedores, terceros o aliados que manipulen datos asociados a soluciones de IA de SOLTEG.

10.3 Responsabilidades

10.3.1. Líder de Órgano Interno de Control:

- Definir los lineamientos y controles de calidad de datos aplicables a todos los sistemas de IA.
- Asegurar que exista un marco de gobernanza de datos alineado a la regulación y al SGIA.
- Aprobar criterios y metodologías de evaluación de calidad de datasets.

10.3.2. Data Owner (Dueño del Dato):

- Definir el uso permitido de los datos bajo su responsabilidad.
- Garantizar la exactitud, integridad, disponibilidad y actualización de los datos.
- Aprobar transformaciones, normalizaciones y definiciones de metadatos.

10.3.3. Data Steward (Custodio del Dato):

- Asegurar la adecuada administración, documentación, trazabilidad y almacenamiento de los datos.
- Implementar los controles de calidad, seguridad y acceso definidos en esta política.
- Monitorear desviaciones o problemas de calidad.

10.3.4. Líderes de Desarrollo de IA y Operación y Soporte de Sistemas de IA:

- Verificar la calidad, relevancia, representatividad y ausencia de sesgos indebidos en los datasets.
- Documentar procesos de limpieza, preparación, etiquetado, enriquecimiento y transformación.
- Asegurar la reproducibilidad de experimentos, modelos y pipelines de datos.

10.3.5. Auditor Interno:

- Validar que los controles de calidad y manejo de datos sean implementados correctamente.
- Verificar trazabilidad, documentación, cumplimiento de políticas y gestión del riesgo de datos.

10.3.6. Proveedores Externos y Terceros:

- Cumplir con estándares de calidad de datos establecidos por SOLTEG.
- Proporcionar evidencia de origen, licenciamiento, limpieza, representatividad y conformidad legal de los datos entregados.

GRIJALVA TECNOLOGÍA

10.4 Generalidades

10.4.1 Los datos utilizados en modelos de IA deben cumplir como mínimo, con los siguientes atributos de calidad:

- Exactitud
- Completitud
- Consistencia
- Actualidad
- Relevancia
- Representatividad
- Ausencia de sesgos indebidos
- Trazabilidad verificable

10.4.2. Lineamientos para datasets de IA:
Cada dataset deberá contar con:

- Metadatos documentados (origen, estructura, licencias, propósito, restricciones).
- Evidencia de revisiones de calidad.
- Validación de sesgos potenciales.
- Pruebas de balance, diversidad y adecuación al caso de uso.

10.4.3. Calidad por diseño:
La preparación de datos deberá incorporar mecanismos para:

- Reducir sesgos no deseados.
- Garantizar seguridad y privacidad por diseño.
- Asegurar que los datos sean apropiados para los modelos utilizados.
- Evitar el uso de datasets corruptos, incompletos o no autorizados.

10.4.4. Trazabilidad del flujo de datos:
Toda manipulación de datos utilizada en los sistemas de IA deberá ser registrada, garantizando la trazabilidad integral del proceso, incluyendo:

- Origen del dato
- Procesos y transformaciones aplicadas
- Versiones del conjunto de datos y del modelo
- Usuarios o sistemas que intervinieron
- Fecha, hora y finalidad del procesamiento

10.4.5. Cumplimiento normativo:
Los datos deberán gestionarse conforme a:

- Normativa de protección de datos personales
- Requisitos contractuales con clientes o proveedores

- Estándares técnicos y de seguridad aplicables
- Requisitos del SGIA e ISO/IEC 42001

10.4.6. Uso ético y proporcional de datos:
Se prohíbe utilizar datos obtenidos sin consentimiento, de fuentes dudosas o empleados de manera discriminatoria, manipuladora o contraria a principios éticos.

10.4.7. Eliminación segura de datos:
Los datos que ya no sean necesarios deberán ser eliminados o anonimizados mediante prácticas seguras y verificables.

10.4.8 Se prohíbe el uso de datos no autorizados o de origen incierto.

11. Política de Seguridad y Ciberseguridad en IA

11.1 Objetivos

Establecer los lineamientos, controles y mecanismos necesarios para garantizar la protección, resiliencia, confidencialidad, integridad, disponibilidad y uso seguro de los sistemas de inteligencia artificial y los activos asociados (modelos, datos, algoritmos, infraestructura y procesos). Así como mitigar riesgos de ciberseguridad y evitar amenazas que puedan comprometer el funcionamiento, la confiabilidad, la ética y el cumplimiento normativo del sistema de SOLTEG.

11.2 Alcance

Esta política aplica a todos los sistemas de IA desarrollados, adquiridos, operados o administrados por SOLTEG, modelos, datasets, algoritmos, APIs, hardware, plataformas, pipelines y entornos utilizados en cualquier fase del ciclo de vida de IA. Áreas, personal interno, proveedores, consultores y terceros que tengan acceso o participen en la operación, mantenimiento, integración o uso de sistemas de IA y Controles de seguridad física, lógica, de red, de infraestructura en la nube, y de protección de datos críticos utilizados por los modelos de IA.

11.3 Responsabilidades

11.3.1. Líder de Órgano Interno de Control:

- Definir los lineamientos de seguridad específicos para sistemas de IA.
- Asegurar la adopción de controles de seguridad basados en riesgos.
- Supervisar el diseño seguro y la protección de modelos, datos y pipelines.

11.3.2. Líder de Infraestructura y Seguridad de IA:

- Implementar controles de seguridad alineados con la ISO/IEC 27001, 27002 y buenas

prácticas de seguridad de IA.
- Monitorear vulnerabilidades, amenazas, intentos de intrusión y anomalías.
- Coordinar análisis de riesgo y pruebas de penetración en sistemas de IA.

11.3.3. Equipos de Desarrollo, Infraestructura y Operaciones de IA:
- Implementar prácticas de "Seguridad por Diseño" y "Privacy by Design".
- Proteger claves, credenciales, modelos, APIs y entornos de ejecución.
- Aplicar controles de acceso, auditoría y monitoreo continuo.

11.3.4. Líder de Soporte Técnico:
- Gestionar incidentes de seguridad relacionados con IA.
- Asegurar parches, actualizaciones y configuraciones seguras.
- Garantizar la continuidad operativa y respaldos adecuados de modelos y datos.

11.3.5. Auditor Interno:
- Verificar el cumplimiento de los controles de seguridad y ciberseguridad.
- Revisar trazabilidad, registros, bitácoras y mecanismos de respuesta a incidentes.
- Recomendar mejoras conforme a los resultados de auditorías.

11.3.6. Recursos Humanos:
- Asegurar que el personal reciba capacitación en ciberseguridad, seguridad de IA y manejo seguro de datos.

11.3.7. Proveedores y terceros:
- Cumplir con los requerimientos de seguridad establecidos en SOLTEG.
- Proporcionar evidencia de controles aplicados a plataformas, datasets o servicios de IA.

11.4 Generalidades

11.4.1. Seguridad por diseño (Security by Design):
Todos los sistemas de IA deben ser diseñados e implementados considerando seguridad desde su concepción, incluyendo:
- controles de acceso estrictos,
- separación de ambientes,
- protección de modelos,
- validación de entradas y salidas,
- monitoreo continuo.

11.4.2. Protección de modelos de IA:

Se deben implementar controles para prevenir:

- robo o replicación de modelos,
- ataques de inversión de modelo,
- ataques adversariales,
- manipulación de parámetros o pesos,
- extracción de información sensible a partir del modelo.

11.4.3. Seguridad de datos utilizados por IA:
Los datos deben estar protegidos mediante:

- cifrado en tránsito y en reposo,
- controles de integridad,
- anonimización o seudonimización cuando aplique,
- control de accesos mínimos necesarios.

11.4.4. Prevención de ataques adversariales:
Se deben evaluar y mitigar amenazas específicas de IA como:

- poisoning (datos maliciosos en entrenamiento),
- evasion attacks,
- prompt injection,
- manipulación de salidas,
- explotación de vulnerabilidades en APIs o inferencias.

11.4.5. Gestión de vulnerabilidades:
Los modelos, bibliotecas, frameworks y pipelines deberán ser evaluados con herramientas y pruebas periódicas para detectar vulnerabilidades o configuraciones inseguras.

11.4.6. Continuidad del negocio y resiliencia:
Los sistemas de IA deberán contar con:

- planes de continuidad,
- respaldos regulares,
- redundancia en componentes críticos,
- planes de recuperación ante desastres o fallas de IA.

11.4.7. Respuesta a incidentes de IA:
Debe existir un proceso documentado para:

- identificar incidentes,
- analizarlos,
- contenerlos,
- recuperarse y
- aplicar lecciones aprendidas.

GRIJALVA TECNOLOGÍA

11.4.8. Cumplimiento normativo:
SOLTEG deberá cumplir con:

- ISO/IEC 42001,
- ISO/IEC 27001/27002 (seguridad de la información),
- ISO/IEC 23894 (riesgos de IA),

ISO/IEC 22989,

- leyes aplicables de protección de datos personales,
- contratos con clientes o terceros.

12. Política de Transparencia y Explicabilidad

12.1 Objetivos

Establecer los lineamientos para garantizar que los sistemas de inteligencia artificial operen con niveles adecuados de transparencia, explicabilidad y trazabilidad, permitiendo que usuarios, operadores, auditores y partes interesadas comprendan el propósito, funcionamiento, limitaciones, riesgos y criterios de decisión de los modelos de IA, promoviendo confianza, responsabilidad y cumplimiento regulatorio.

12.2 Alcance

Esta política aplica a todos los sistemas, modelos, algoritmos y soluciones de IA desarrollados o utilizados por SOLTEG, procesos de documentación, evaluación, despliegue y operación que requieran explicar decisiones o resultados generados por IA, así como al personal interno, proveedores y terceros involucrados en el diseño, validación, operación y supervisión de sistemas de IA; Usuarios internos y externos que interactúan con funcionalidades automatizadas o semiautomatizadas basadas en IA y cualquier componente del ciclo de vida de IA en el que sea necesario documentar trazabilidad, lógica, criterios, limitaciones o factores de riesgo del sistema.

12.3 Responsabilidades

12.3.1. Líder de Órgano Interno de Control / (Líder de Órgano Interno de Control):

- Definir los criterios institucionales de transparencia y explicabilidad requeridos según el nivel de riesgo del sistema.
- Asegurar que cada sistema de IA cuente con documentación suficiente sobre propósito, diseño, datos, funcionamiento y limitaciones.
- Verificar que los mensajes y explicaciones ofrecidas a los usuarios sean claros, útiles y apropiados para el público objetivo.

12.3.2. Equipos de Desarrollo, Datos e Infraestructura:

• Documentar arquitectura, datasets utilizados, algoritmos, parámetros clave, procesos de entrenamiento y validación.
• Garantizar que los modelos de IA incluyan mecanismos de trazabilidad y registros de decisiones.
• Implementar herramientas o técnicas que permitan generar explicaciones técnicas y no técnicas (ej. saliency maps, LIME, SHAP, resumen de reglas, metadatos de decisiones).

12.3.3. Director de Operaciones y Líder de Operaciones y Soporte de Sistemas de IA:
• Asegurar que los usuarios internos y externos reciban información adecuada sobre cómo funciona la IA dentro de los procesos en los que interactúan.
• Proveer canales para atender dudas, solicitudes de explicación o aclaración derivadas del uso de IA.

12.3.4. Auditor Interno:
• Verificar que los mecanismos de transparencia, explicabilidad y trazabilidad se encuentren documentados, actualizados y aplicados en cada sistema de IA.
• Evaluar que la información proporcionada a usuarios y partes interesadas sea suficiente y coherente con la normativa.

12.3.5. Recursos Humanos:
• Asegurar que el personal reciba capacitación básica sobre transparencia, explicabilidad y comunicación ética en IA.

12.3.6. Proveedores y terceros:
• Proveer documentación clara sobre modelos, algoritmos, APIs o soluciones de IA que suministren a SOLTEG.
• Permitir el acceso a información necesaria para auditorías, revisiones o evaluaciones de transparencia y explicabilidad.

12.4 Generalidades

12.4.1. Documentación obligatoria de cada sistema de IA:
Debe incluir como mínimo:
• propósito y alcance,
• nivel de riesgo,
• arquitectura y componentes,
• descripción de datasets,
• supuestos y limitaciones,
• criterios de decisión,
• métricas de rendimiento,
• mecanismos de supervisión humana.

12.4.2. Trazabilidad del ciclo de vida de IA:

Se debe mantener un registro auditable de:

- decisiones del modelo,
- fuentes de datos,
- cambios realizados al modelo o dataset,
- versiones del modelo,
- evidencias de validación y pruebas.

12.4.3. Explicabilidad adecuada al nivel de riesgo:

- IA de alto riesgo requiere explicaciones técnicas robustas y documentación profunda.
- IA de impacto moderado requiere explicaciones comprensibles para operadores y auditores.
- IA de bajo riesgo requiere información mínima adecuada al usuario final.

12.4.4. Comunicación clara hacia los usuarios:
Todos los sistemas de IA deben informar al usuario final cuando estén interactuando con IA, incluyendo:

- finalidad del sistema,
- límites,
- posibles errores,
- cómo solicitar asistencia humana.

12.4.5. Accesibilidad de la información:
Las explicaciones deberán ser:

- comprensibles,
- verificables,
- oportunas,
- adaptadas al público destinatario (técnico o no técnico).

12.4.6. Restricciones de transparencia:
La transparencia no debe comprometer:

- seguridad del sistema,
- propiedad intelectual,
- información sensible o confidencial,
- modelos vulnerables a ataques por divulgación excesiva.

12.4.7. Cumplimiento normativo:
SOLTEG deberá garantizar transparencia y explicabilidad conforme a:

- ISO/IEC 42001,
- ISO/IEC 22989,

- ISO/IEC 23894,
- leyes de protección de datos y derechos de los usuarios,
- regulaciones sectoriales aplicables.

13. Política de Supervisión Humana

SOLTEG reconoce que la supervisión humana es indispensable para asegurar que los sistemas de Inteligencia Artificial (IA) operen de manera segura, ética y alineada con los objetivos institucionales. Esta política establece los lineamientos para garantizar que las personas mantengan el control significativo sobre los sistemas de IA, especialmente en aquellos clasificados como de riesgo medio o alto, conforme a los criterios de clasificación establecidos en el SGIA.

13.1 Objetivo

Establecer los principios, directrices y mecanismos que aseguren una supervisión humana efectiva, oportuna y documentada durante todo el ciclo de vida de los sistemas de IA, con el fin de prevenir y mitigar riesgos derivados del uso y operación de sistemas de IA, garantizando que los seres humanos puedan entender, monitorear e intervenir cuando sea necesario, así como asegurar decisiones responsables y trazables en los procesos automatizados o asistidos por IA y mantener el control significativo sobre los sistemas de IA, evitando dependencias excesivas o automatización no verificada.

13.2 Alcance

Esta política aplica a:

- Todos los sistemas de IA existentes, en desarrollo o en proceso de adquisición dentro de SOLTEG, colaboradores que desarrollan, operan, administran, evalúan o utilizan sistemas de IA., proveedores externos, socios tecnológicos y terceros cuyas soluciones de IA tengan impacto en operaciones, servicios o datos de SOLTEG, todas las etapas del ciclo de vida de IA: diseño, desarrollo, implementación, validación, operación, mantenimiento, monitoreo y retiro.

13.3 Responsabilidades

13.3.1 Líder de Órgano Interno de Control:

- Establecer los criterios para determinar el nivel de supervisión requerido según el riesgo del sistema.
- Monitorear el cumplimiento de esta política y reportar desviaciones.

- Revisar la eficacia de los mecanismos de supervisión humana.

13.3.2 Propietarios del Sistema de IA

- Definir puntos de control, umbrales de alerta y condiciones que requieran intervención humana.
- Asegurar que el personal asignado tenga competencias necesarias.
- Validar que los outputs del sistema sean adecuados antes de utilizarse en decisiones críticas.

13.3.3 Usuarios Operativos

- Desempeñar la supervisión asignada siguiendo los procedimientos establecidos.
- Reportar comportamientos inesperados, sesgos, errores o riesgos detectados en el sistema.
- Abstenerse de delegar completamente decisiones sensibles sin validación humana.

13.3.4 Área de TI / Ciberseguridad

- Asegurar que existan logs, trazas y mecanismos de auditoría que permitan supervisión efectiva.
- Implementar salvaguardas técnicas para permitir intervención humana segura.

13.3.5 Proveedores y Terceros

- Proveer documentación y funcionalidades que apoyen la supervisión humana, incluyendo controles de intervención y explicación operativa.

13.4 Generales

13.4.1 Todos los sistemas de IA deberán incorporar mecanismos de control humano, tales como revisión de decisiones, validación manual, doble verificación o aprobación por expertos.

13.4.2 Todos los sistemas de IA deberán incorporar mecanismos de control humano, tales como revisión de decisiones, validación manual, doble verificación o aprobación por expertos.

13.4.3 La intervención humana deberá ser posible en cualquier momento, especialmente ante comportamientos anómalos o resultados inesperados.

13.4.4 Se deberán establecer umbrales de riesgo que indiquen automáticamente cuándo un humano debe validar, detener o ajustar el funcionamiento del sistema.

13.4.5 Los sistemas de alto riesgo deberán contar con procedimientos de “parada segura” (safe stop) operables por personal autorizado.

13.4.6 Toda supervisión humana deberá quedar documentada mediante registros operativos, auditorías internas o controles del SGIA.

13.4.7 El entrenamiento del personal será obligatorio para asegurar comprensión del sistema, posibles sesgos y limitaciones.

13.4.8. Se deberá garantizar que los sistemas no generen situaciones donde las decisiones críticas se tomen sin revisión humana cuando así lo requiera el nivel de riesgo.

13.4.9 SOLTEG promoverá una cultura de responsabilidad, fomentando que los usuarios reporten fallas o riesgos sin temor a represalias.

13.4.10 La supervisión humana será revisada de forma periódica para evaluar su eficacia y realizar mejoras continuas.

13.4.11 Se deberán establecer umbrales de riesgo que indiquen automáticamente cuándo un humano debe validar, detener o ajustar el funcionamiento del sistema.

13.4.12 Todos los sistemas de IA deberán incorporar mecanismos de control humano, tales como revisión de decisiones, validación manual, doble verificación o aprobación por expertos.

13.4.13 La intervención humana deberá ser posible en cualquier momento, especialmente ante comportamientos anómalos o resultados inesperados.

13.4.14 Se deberán establecer umbrales de riesgo que indiquen automáticamente cuándo un humano debe validar, detener o ajustar el funcionamiento del sistema.

13.4.15 Los sistemas de alto riesgo deberán contar con procedimientos de “parada segura” (safe stop) operables por personal autorizado.

13.4.16 Toda supervisión humana deberá quedar documentada mediante registros operativos, auditorías internas o controles del SGIA.

13.4.17 El entrenamiento del personal será obligatorio para asegurar comprensión del sistema, posibles sesgos y limitaciones.

13.4.18 Se deberá garantizar que los sistemas no generen situaciones donde las decisiones críticas se tomen sin revisión humana cuando así lo requiera el nivel de riesgo.

13.4.19 SOLTEG promoverá una cultura de responsabilidad, fomentando que los usuarios reporten fallas o riesgos sin temor a represalias.

13.4.20 La supervisión humana será revisada de forma periódica para evaluar su eficacia y realizar mejoras continuas.

14. Política de Privacidad y Protección de Datos

SOLTEG reconoce que la protección de los datos personales y sensibles utilizados en sistemas de Inteligencia Artificial (IA) es fundamental para preservar los derechos de las personas, fortalecer la confianza en el uso de estas tecnologías y cumplir con la normativa vigente. Esta política establece los lineamientos para asegurar que el tratamiento de datos dentro del ciclo de vida de los sistemas de IA se realice de manera lícita, ética, segura, transparente y proporcional, aplicando medidas técnicas y organizativas que garanticen su confidencialidad, integridad y disponibilidad, así como la prevención de riesgos que puedan afectar la privacidad de los titulares.

14.1 Objetivos

Establecer los lineamientos que aseguren que el tratamiento de datos personales y datos sensibles en los sistemas de Inteligencia Artificial (IA) se realice de forma lícita, ética, transparente y segura, garantizando la protección de los derechos de los titulares, el cumplimiento de la legislación aplicable, la minimización de riesgos asociados al uso indebido de los datos, y la implementación de medidas técnicas y organizativas que salvaguarden su confidencialidad, integridad y disponibilidad durante todo el ciclo de vida de los sistemas de IA.

14.2 Alcance

Esta política aplica a todos los sistemas de IA utilizados, desarrollados, operados o gestionados por SOLTEG, así como a cualquier tratamiento de datos personales y sensibles realizado durante las actividades de diseño, recolección, preparación, entrenamiento, evaluación, despliegue, monitoreo y retiro de modelos de IA, incluyendo a todas las áreas internas, terceros, proveedores, socios tecnológicos, usuarios operativos y cualquier persona que tenga acceso, gestione o procese datos en el contexto del SGIA.

GRIJALVA TECNOLOGÍA

14.3 Responsabilidades

14.3.1 Líder de Órgano Interno de Control:

- Supervisar la implementación de controles de privacidad dentro de los sistemas de IA.
- Validar que los datos utilizados cumplan con requisitos legales y regulatorios.
- Monitorear riesgos de privacidad y proponer mejoras continuas.

14.3.2 Consejería Jurídica

- Asegurar el cumplimiento de las leyes de protección de datos personales aplicables.
- Revisar y aprobar evaluaciones de impacto en privacidad (PIA).
- Emitir lineamientos para el manejo de datos sensibles y transferencia de información.

14.3.3 Área de TI

- Implementar medidas técnicas de seguridad, incluyendo cifrado, control de accesos y monitoreo.
- Asegurar que las plataformas utilizadas para IA protejan los datos durante todo su ciclo de vida.

14.3.4 Propietarios del Sistema de IA

- Verificar que los datos utilizados para entrenamiento, validación y operación sean adecuados, pertinentes y mínimos.
- Garantizar la eliminación segura de datos cuando ya no sean necesarios.

14.3.5 Usuarios Operativos

- Utilizar únicamente la información autorizada según su función.
- Reportar incidentes, accesos indebidos o posibles vulneraciones de datos.

14.3.6 Proveedores y Terceros

- Cumplir con los requisitos de privacidad establecidos contractualmente.
- Proporcionar garantías técnicas y organizativas para proteger los datos gestionados por sus servicios o tecnologías.

14.4 Generalidades

14.4.1 Todo tratamiento de datos personales en sistemas de IA deberá seguir los principios de licitud, finalidad, proporcionalidad, minimización y exactitud.

14.4.2 Los sistemas de IA deberán evitar el uso de datos sensibles salvo que sea estrictamente necesario y bajo controles reforzados.

14.4.3 Antes de desarrollar o desplegar un sistema de IA, deberá elaborarse una Evaluación de Impacto en Privacidad (PIA).

14.4.4 Se deberán aplicar técnicas de protección de datos como anonimización, pseudoanonimización o agregación cuando sea viable.

14.4.5 Los modelos de IA deberán ser entrenados únicamente con datos autorizados y con salvaguardas para evitar sesgos y discriminación.

14.4.6 Todo incidente que comprometa datos personales deberá reportarse y gestionarse conforme al procedimiento de respuesta a incidentes.

14.4.7 SOLTEG deberá establecer controles de retención y eliminación segura de datos utilizados en IA.

14.4.8 Los derechos de los titulares (acceso, rectificación, cancelación, oposición, portabilidad) deberán ser respetados en la operación de sistemas de IA.

14.4.9 Esta política será revisada periódicamente y actualizada conforme a cambios tecnológicos, regulatorios o de riesgos.

15. Política de Gestión de Proveedores y Terceros

SOLTEG reconoce que los proveedores, aliados tecnológicos y terceros que participan en el diseño, desarrollo, implementación, operación o mantenimiento de sistemas de Inteligencia Artificial (IA) representan elementos críticos dentro del SGIA, por lo que su adecuada gestión es esencial para asegurar que las prácticas, tecnologías y servicios proporcionados se alineen con los principios de seguridad, ética, transparencia, calidad y gobernanza establecidos. Esta política define los lineamientos para evaluar, seleccionar, monitorear y controlar a proveedores y terceros, garantizando que cumplan con los requisitos normativos, contractuales y técnicos necesarios para mitigar riesgos y asegurar la operación responsable y confiable de los sistemas de IA.

15.1 Objetivo

Establecer los criterios, controles y procedimientos necesarios para gestionar

adecuadamente a proveedores y terceros involucrados en cualquier etapa del ciclo de vida de los sistemas de IA, asegurando que sus servicios, tecnologías, modelos, datos y herramientas cumplan con los estándares del SGIA, la normativa vigente, los requisitos de seguridad y privacidad, y los principios éticos y de gobernanza establecidos por SOLTEG, con el fin de mitigar riesgos y garantizar que la colaboración externa sea confiable, segura y alineada con los objetivos institucionales.

15.2 Alcance

Esta política aplica a todos los proveedores, contratistas, consultores, aliados tecnológicos, terceros externos y entidades que proporcionen servicios, modelos, datasets, infraestructura, herramientas, desarrollos, componentes o soporte relacionado con sistemas de IA, abarcando todas las etapas del ciclo de vida, desde la adquisición y evaluación inicial hasta el monitoreo continuo, renovación o terminación de la relación contractual, incluyendo a todas las áreas internas que gestionen o interactúen con dichos terceros en el marco del SGIA.

15.3 Responsabilidades

15.3.1 Líder de Órgano Interno de Control

Evaluar y aprobar los criterios de selección, monitoreo y control de proveedores y terceros relacionados con IA, así como supervisar su cumplimiento con los lineamientos establecidos en esta política.

15.3.2 Área de Compras

Registrar, evaluar y seleccionar proveedores siguiendo los criterios definidos para IA, asegurar que los contratos incluyan cláusulas de cumplimiento con el SGIA y dar seguimiento a su desempeño.

15.3.3 Director de Operaciones

Garantizar que los proveedores tecnológicos cumplan con los requisitos técnicos, operativos y de seguridad, así como supervisar que los servicios prestados sean coherentes con las necesidades del sistema de IA.

15.3.4 Área de TI / Ciberseguridad

Verificar que los proveedores implementen controles de seguridad adecuados, gestionar evaluaciones de vulnerabilidades en servicios o modelos proporcionados y monitorear riesgos asociados.

15.3.5 Propietarios del Sistema de IA

Validar que los proveedores cumplan con las especificaciones técnicas del sistema, supervisar su desempeño y reportar incidentes o desviaciones relacionadas con la calidad o

GRIJALVA TECNOLOGÍA

seguridad del servicio.

15.3.6 Proveedores y Terceros
Cumplir con los requisitos establecidos por SOLTEG en materia de seguridad, privacidad, gobernanza y calidad, además de proporcionar documentación adecuada y reportar cualquier irregularidad detectada.

15.4 Generalidades

15.4.1 Todos los proveedores deberán ser evaluados mediante criterios objetivos de riesgo, impacto, seguridad, privacidad y confiabilidad antes de su contratación.

15.4.2 Los contratos con terceros deberán incluir cláusulas sobre protección de datos, confidencialidad, seguridad, gobernanza de IA y cumplimiento del SGIA.

15.4.3 SOLTEG deberá mantener un registro actualizado de todos los proveedores vinculados a sistemas de IA, incluyendo niveles de riesgo y evidencias de cumplimiento.

15.4.4 Los servicios proporcionados por terceros deberán ser monitoreados regularmente mediante auditorías, revisiones técnicas o análisis de desempeño.

15.4.5 Ningún proveedor podrá operar o suministrar componentes críticos de IA sin una evaluación previa de riesgo conforme al SGIA.

15.4.6 En caso de desviaciones, incidentes o incumplimientos, se deberán activar medidas de corrección, suspensión o terminación conforme a los procedimientos internos.

15.4.7 Los proveedores de alto riesgo deberán proporcionar evidencia documental adicional, como reportes de seguridad, pruebas de sesgos o evaluaciones de impacto.

15.4.8 SOLTEG deberá asegurar que los proveedores respeten los principios éticos y de uso responsable de IA establecidos en el SGIA.

15.4.9 Se promoverá la mejora continua en la cadena de suministro, incentivando a los proveedores a adoptar buenas prácticas y estándares internacionales aplicables.

GRIJALVA TECNOLOGÍA

16. Política de Incidentes y No Conformidades de IA

SOLTEG establece esta política para asegurar que todos los incidentes, desviaciones, fallas, anomalías y no conformidades relacionadas con los sistemas de Inteligencia Artificial sean identificados, registrados, investigados, gestionados y resueltos de manera oportuna y efectiva, garantizando la operación segura, confiable, ética y conforme a los requisitos legales, normativos y del SGIA, así como la mejora continua del desempeño de los sistemas de IA y de los procesos asociados.

16.1 Objetivo

Definir los lineamientos para la atención sistemática de incidentes y no conformidades en los sistemas de IA, asegurando su detección temprana, correcta clasificación, análisis de causa raíz, implementación de acciones correctivas o preventivas, y verificación de eficacia, con el fin de prevenir impactos negativos en la seguridad, privacidad, ética, operación, cumplimiento normativo y desempeño técnico de los sistemas de IA.

16.2 Alcance

Esta política aplica a todos los sistemas de Inteligencia Artificial desarrollados, adquiridos, operados o supervisados por SOLTEG, incluyendo modelos, datasets, infraestructuras, proveedores y terceros involucrados, así como al personal interno que interviene en el ciclo de vida de los sistemas de IA. El alcance abarca la gestión de incidentes técnicos, operativos, éticos, de privacidad, ciberseguridad, confiabilidad, desempeño o cumplimiento, sin importar su origen, severidad o área donde se presenten.

16.3 Responsabilidades

16.3.1 Líder de Órgano Interno de Control.

- Dirigir la gestión integral de incidentes y no conformidades.
- Validar acciones correctivas y cerrar incidentes mayores.
- Informar al Comité de Gobernanza de IA sobre incidentes significativos.

16.3.2 Líder de Órgano Interno de Control.

- Verificar que la gestión se realice conforme al proceso y a la norma ISO/IEC 42001.
- Confirmar trazabilidad, evidencia y cierre adecuado de no conformidades.
- Escalar incidentes que representen incumplimientos o riesgos relevantes.

16.3.3 Responsable de Seguridad de la Información

- Atender incidentes de ciberseguridad, integridad de datos y fallas técnicas críticas.
- Coordinar acciones inmediatas de contención y mitigación.
- Documentar evidencia técnica.

16.3.4 líder de Desarrollo de IA y Líder de Riesgos y control del SGIA

- Gestionar incidentes que involucren datos personales.
- Evaluar impactos a la privacidad y coordinar notificaciones regulatorias en caso aplicable.
- Emitir acciones de mitigación relacionadas con protección de datos.

16.3.5 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Detectar y reportar anomalías o comportamientos inesperados.
- Implementar acciones correctivas asignadas.
- Registrar evidencias de pruebas posteriores.

16.3.6 Propietarios de Sistemas de IA (System Owners)

- Coordinar recursos y actividades para resolver incidentes en su área.
- Evitar la operación de sistemas afectados por incidentes críticos.
- Asegurar que modelos o versiones no se liberen con desviaciones activas.

16.3.7 Comité de Gobernanza de IA

- Revisar incidentes mayores y sus implicaciones estratégicas.
- Solicitar controles adicionales cuando el incidente lo amerite.
- Aprobar acciones correctivas de impacto transversal.

16.4 Generalidades

16.4.1 Todo incidente o no conformidad debe registrarse de forma inmediata y documentarse con evidencia.

16.4.2 Se debe aplicar clasificación por severidad e impacto para priorizar la atención.

16.4.3 Ningún sistema podrá operar si existe un incidente crítico sin atender.

16.4.4 Debe realizarse análisis de causa raíz e implementar acciones correctivas verificables.

16.4.5 Las lecciones aprendidas deben integrarse al proceso de mejora continua del SGIA.

16.4.6 La trazabilidad completa del ciclo del incidente debe mantenerse como evidencia.

16.4.7 Se garantizará la comunicación oportuna a las autoridades internas y externas correspondientes, cuando aplique

GRIJALVA TECNOLOGÍA

17. Política de Monitoreo y Desempeño de Modelos

SOLTEG establece esta política para garantizar que todos los modelos de Inteligencia Artificial implementados sean monitoreados continuamente para asegurar su desempeño, estabilidad, precisión, equidad, seguridad y confiabilidad, permitiendo detectar desviaciones, degradación, sesgos emergentes o fallas operativas, y asegurar que los modelos mantengan niveles de desempeño alineados con los requisitos del SGIA, los objetivos institucionales y las regulaciones aplicables.

17.1 Objetivos

Definir los lineamientos que aseguren el monitoreo sistemático, medible y constante del desempeño de los modelos de IA, mediante métricas técnicas, operativas, éticas y de riesgo, con el fin de identificar y corregir degradaciones, asegurar consistencia en los resultados, mantener la vigencia del modelo, prevenir impactos negativos y garantizar que su operación continúe siendo segura, confiable y conforme al marco normativo.

17.2 Alcance

Aplica a todos los modelos de IA desarrollados, entrenados, adquiridos, operados o supervisados por SOLTEG, incluyendo modelos predictivos, clasificadores, algoritmos de toma de decisiones, sistemas generativos, modelos embebidos en proveedores externos y cualquier componente que influya en el resultado del sistema. Así como las actividades de monitoreo técnico, auditoría de desempeño, evaluación de sesgo, revisión periódica, pruebas de estabilidad y verificación de métricas operativas.

17.3 Responsabilidades

17.3.1 Líder de Órgano Interno de Control.

- Supervisar el cumplimiento de los lineamientos de monitoreo definidos en esta política.
- Validar los reportes de desempeño y aprobar acciones de mejora en modelos de alto impacto.
- Presentar resultados al Comité de Gobernanza de IA.

17.3.2 Líder de Órgano Interno de Control.

- Verificar que el monitoreo se realice conforme a la norma ISO/IEC 42001.
- Auditar la confiabilidad de las métricas, evidencias y reportes de desempeño.
- Escalar desviaciones críticas que representen riesgo o incumplimiento.

17.3.3 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Implementar procesos de monitoreo continuo de modelos (drift, accuracy, fairness, estabilidad).
- Analizar comportamientos anómalos y proponer acciones correctivas.
- Mantener trazabilidad de versiones, métricas y experimentos del modelo.

17.3.4 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Evaluar periódicamente si el desempeño del modelo sigue siendo adecuado para su propósito.
- Coordinar recursos para reentrenamientos o ajustes cuando el desempeño disminuya.
- Aprobar la liberación de nuevas versiones del modelo en producción.

17.3.5 Líder de Infraestructura y Seguridad de IA

- Detectar posibles ataques, manipulación de datos o adversarial inputs que afecten el desempeño.
- Proponer controles de seguridad que protejan la integridad del modelo.

17.3.6 Proveedores y Terceros

- Proveer métricas, documentación técnica y evidencia del desempeño de los modelos externos.
- Notificar oportunamente sobre degradaciones, parches o vulnerabilidades detectadas.

17.4 Generalidades

17.4.1 Todos los modelos deberán contar con métricas claras, medibles y documentadas de desempeño, alineadas a su propósito.

17.4.2 Se deberán implementar mecanismos de monitoreo continuo para detectar drift, sesgos emergentes o disminución de precisión.

17.4.3 Los modelos deben someterse a revisiones periódicas que incluyan pruebas de estrés, estabilidad y equidad.

17.4.4 Ningún modelo podrá operar en producción si sus métricas caen por debajo de los umbrales definidos.

17.4.5 Todo cambio, ajuste o reentrenamiento deberá documentarse y conservar trazabilidad técnica y operativa.

17.4.6 Los indicadores clave de desempeño (KPIs) deben revisarse y actualizarse cuando el contexto operacional o regulatorio cambie.

17.4.7 Los resultados del monitoreo formarán parte del ciclo de mejora continua del SGIA.

18. Política de Competencia y Capacitación

18.1 Objetivos

Asegurar el desarrollo, fortalecimiento y actualización continua de las competencias del personal relacionado con IA, mediante programas de capacitación estructurados, certificaciones, evaluaciones periódicas, sensibilización en temas éticos y regulatorios, y mecanismos que garanticen que las personas comprendan los riesgos, limitaciones, implicaciones y responsabilidades asociadas al uso de IA en SOLTEG.

18.2 Alcance

Esta política aplica a todos los colaboradores, directivos, auditores, operadores, desarrolladores, analistas, administradores de sistemas, responsables de seguridad, proveedores y terceros que intervengan directa o indirectamente en procesos, decisiones o actividades relacionadas con el ciclo de vida de sistemas de IA. Incluye capacitación inicial, continua, especializada, certificaciones, evaluaciones de competencia y actividades para garantizar la alfabetización digital y ética en IA.

18.3 Responsabilidades

18.3.1 Líder de Órgano Interno de Control.

- Establecer el marco general de competencias requeridas para los roles vinculados a IA.
- Validar los programas de capacitación y su alineación con las normas ISO/IEC 42001 e ISO 22989.
- Supervisar el cumplimiento de los planes anuales de entrenamiento.

18.3.2 Líder de Órgano Interno de Control.

- Verificar que las capacitaciones obligatorias se realicen y cuenten con evidencia

documental.

- Auditar la eficacia de los programas de formación relacionados con riesgos y ética de IA.
- Reportar desviaciones o incumplimientos en materia de competencias.

18.3.3 Gerencia de Recursos Humanos

- Diseñar, planear y coordinar los programas de formación interna y externa.
- Mantener registros actualizados de competencias, constancias, evaluaciones y certificaciones.
- Asegurar que el personal recién incorporado reciba capacitación inicial en SGIA e IA responsable.

18.3.4 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Definir los conocimientos técnicos específicos requeridos para los roles de desarrollo y operación de IA.
- Impartir capacitaciones especializadas y sesiones de transferencia de conocimiento.
- Evaluar la competencia técnica del personal asignado a proyectos de IA.

18.3.5 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Identificar brechas de competencia dentro de su equipo y solicitar capacitación necesaria.
- Verificar que los usuarios operativos comprendan los límites, riesgos y controles del sistema.
- Asegurar que las personas asignadas a actividades críticas cuenten con habilidades suficientes.

18.3.6 Usuarios Operativos

- Participar en los programas de capacitación obligatorios y evaluaciones de competencia.
- Aplicar los conocimientos adquiridos en el uso adecuado del sistema de IA.
- Reportar necesidades adicionales de capacitación o dudas sobre el funcionamiento del sistema.

18.3.7 Proveedores y Terceros

- Proporcionar documentación, formación técnica o sesiones especializadas cuando su tecnología sea utilizada.
- Garantizar que su personal asignado a SOLTEG sea competente para actividades vinculadas a IA.

18.4 Generalidades

18.4.1 SOLTEG establecerá un plan anual de capacitación en IA, ética, riesgo, ciberseguridad y normativa aplicable.

18.4.2 Todo personal involucrado en sistemas de IA deberá acreditar un nivel mínimo de competencia determinado por el SGIA.

18.4.3 Se promoverá la formación continua para atender cambios tecnológicos, regulatorios o de riesgo.

18.4.4 La capacitación incluirá sensibilización sobre sesgos, impacto social, transparencia y supervisión humana.

18.4.5 Se elaborarán perfiles de puesto con competencias específicas para roles críticos en IA.

18.4.6 Las evaluaciones de competencia deberán documentarse y formar parte de los registros del SGIA.

18.4.7 SOLTEG fomentará la profesionalización mediante certificaciones especializadas en IA y SGIA.

18.4.8 El incumplimiento en requisitos de competencia podrá restringir el acceso a sistemas o funciones críticas.

18.4.9 La eficacia del programa de capacitación será evaluada periódicamente como parte de la mejora continua del SGIA.

19. Política de Cumplimiento Legal y Normativo

SOLTEG establece esta política con el propósito de garantizar que todos los sistemas de Inteligencia Artificial (IA), así como las actividades asociadas a su desarrollo, operación, mantenimiento, supervisión y uso, cumplan plenamente con las leyes, regulaciones, estándares nacionales e internacionales, lineamientos éticos y requerimientos contractuales aplicables. Esta política busca asegurar que SOLTEG gestione la IA de manera responsable, transparente y conforme al marco regulatorio vigente, reduciendo riesgos legales, operativos y reputacionales.

19.1 Objetivos

Establecer los lineamientos necesarios para identificar, monitorear, aplicar y mantener el cumplimiento de todas las obligaciones legales, normativas, regulatorias y contractuales asociadas al uso de IA. Asimismo, se busca garantizar que los sistemas de IA operen dentro

de parámetros éticos y de gobernanza que aseguren la protección de derechos humanos, privacidad, seguridad y confianza.

19.2 Alcance

Esta política aplica a todos los colaboradores, directivos, responsables de procesos, desarrolladores, auditores internos, proveedores, asesores legales y terceros que participen en actividades relacionadas con el ciclo de vida de los sistemas de IA. Incluye el cumplimiento de legislación nacional, estándares internacionales como ISO/IEC 42001, ISO 22989, ISO 23894, disposiciones contractuales con terceros, normativas sectoriales, lineamientos gubernamentales y obligaciones en materia de privacidad, seguridad, ética, transparencia y derechos de usuario.

19.3 Responsabilidades

19.3.1 Líder de Órgano Interno de Control.

- Asegurar que los requisitos legales y normativos aplicables al uso de IA se identifiquen, documenten y actualicen periódicamente.
- Coordinar la implementación de controles para cumplir con los marcos regulatorios vigentes.
- Validar que los sistemas de IA operen conforme a los requisitos legales y contractuales.

19.3.2 Líder de Órgano Interno de Control.

- Verificar el cumplimiento regulatorio del SGIA mediante auditorías internas.
- Monitorear desviaciones y emitir recomendaciones para su corrección.
- Asegurar que las obligaciones legales y normativas cuenten con evidencia documental actualizada.

19.3.3 Consejería Jurídica

- Identificar leyes, normas, regulaciones y estándares aplicables al uso de IA.
- Asesorar técnicamente sobre implicaciones legales y riesgos normativos.
- Revisar contratos con proveedores para garantizar cumplimiento en soluciones de IA.

19.3.4 Propietarios del Sistema de IA.

- Garantizar que sus sistemas de IA cumplan con las obligaciones legales y normativas definidas.
- Mantener documentación de versiones, cambios y justificaciones de diseño asociadas al cumplimiento regulatorio.
- Notificar riesgos de incumplimiento o cambios regulatorios que afecten el sistema.

19.3.5 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Aplicar requisitos técnicos derivados de regulaciones (privacidad, explicabilidad, seguridad, retención de datos, etc.).
- Implementar medidas técnicas que garanticen conformidad con estándares de calidad y seguridad.
- Mantener evidencia técnica de cumplimiento en cada etapa del ciclo de vida.

19.3.6 Usuarios Operativos

- Operar los sistemas de IA siguiendo las regulaciones, lineamientos y procedimientos establecidos.
- Reportar cualquier actividad, comportamiento o dato que pueda representar riesgo de incumplimiento.

19.3.7 Proveedores y Terceros

- Garantizar que las soluciones, servicios o modelos proporcionados cumplan con requisitos legales y normativos aplicables.
- Proporcionar documentación, certificaciones o evidencias que respalden conformidad.

19.4 Generalidades

19.4.1 SOLTEG mantendrá un registro actualizado de requisitos legales y normativos aplicables al uso de IA.

19.4.2 Todos los sistemas de IA deberán someterse a revisiones periódicas de cumplimiento regulatorio.

19.4.3 Los cambios legales o regulatorios deberán evaluarse para determinar ajustes necesarios en procesos o sistemas.

19.4.4 El cumplimiento normativo será parte del proceso de gestión de riesgos del SGIA.

19.4.5 Los proveedores deberán demostrar conformidad con obligaciones legales mediante documentación verificable.

19.4.6 El no cumplimiento será tratado como incidente mayor y sujeto a acciones correctivas inmediatas.

19.4.7 Todo el personal deberá recibir capacitación en legislación y regulaciones aplicables a IA.

19.4.8 La evidencia de cumplimiento deberá integrarse en los registros obligatorios del SGIA.

19.4.9 SOLTEG fomentará una cultura de respeto a la ley, transparencia y cumplimiento proactivo.

20. Política de Mejora Continua del SGIA

SOLTEG establece esta política con el propósito de garantizar que el Sistema de Gestión de Inteligencia Artificial (SGIA) evolucione de manera sistemática, consistente y basada en evidencia, mediante procesos de evaluación, retroalimentación, aprendizaje organizacional y optimización continua. Esta política promueve la adaptación del SGIA a cambios tecnológicos, regulatorios, operativos y de riesgo, asegurando que los sistemas de IA mantengan un desempeño seguro, ético, confiable y alineado con los objetivos institucionales.

20.1 Objetivo

Establecer los lineamientos para asegurar que el SGIA se mantenga vigente, eficaz y alineado con las mejores prácticas mediante actividades de revisión, auditoría, retroalimentación, análisis de desempeño, corrección de desviaciones y mejora continua de procesos, modelos, datos y controles asociados al ciclo de vida de los sistemas de IA.

20.2 Alcance

Esta política aplica a todos los procesos, áreas, responsables, sistemas de IA, actividades de operación, documentación, métricas, reportes, auditorías, análisis de riesgos y decisiones asociadas al SGIA. Incluye la participación de todos los roles involucrados en el desarrollo, gestión, operación, supervisión, revisión y mejora de los sistemas de IA, así como a proveedores, terceros, comités de revisión y órganos de control.

20.3 Responsabilidades

20.3.1 Líder de Órgano Interno de Control

- Coordinar y liderar las actividades de mejora continua del SGIA.
- Evaluar la eficacia del sistema, identificar áreas de mejora y proponer acciones correctivas y preventivas.
- Supervisar la implementación de mejoras en modelos, procesos, documentación y controles.

20.3.2 Líder de Órgano Interno de Control.

- Verificar que las acciones de mejora sean implementadas y documentadas.
- Evaluar la consistencia del SGIA con los hallazgos de auditorías internas y revisiones anuales.

20.3.3 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Proponer mejoras basadas en desempeño, incidentes, métricas y retroalimentación de usuarios.
- Implementar mejoras operacionales o técnicas en los sistemas de IA asignados.

20.3.4 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Implementar mejoras técnicas derivadas de evaluaciones, auditorías, análisis de desempeño y cambios normativos.
- Documentar las modificaciones en modelos, datasets, arquitecturas o controles técnicos.

20.3.5 Usuarios Operativos

- Reportar oportunidades de mejora, fallas recurrentes, problemas operativos o limitaciones del sistema.
- Participar en procesos de retroalimentación establecidos por el SGIA.

20.3.6 Proveedores y Terceros

- Incorporar mejoras tecnológicas o prácticas recomendadas en los servicios o soluciones proporcionadas.
- Proveer actualizaciones, parches, documentación y evidencia de mejoras realizadas.

20.4 Generalidades

20.4.1 La mejora continua del SGIA se basará en resultados de auditorías internas, revisiones por la dirección, análisis de desempeño de modelos y evaluación de riesgos.

20.4.2 Toda mejora implementada deberá documentarse como parte de los registros obligatorios del SGIA.

20.4.3 SOLTEG promoverá aprendizaje organizacional mediante revisión de incidentes, no conformidades, métricas y retroalimentación de usuarios.

20.4.4 El SGIA será revisado de manera integral al menos una vez al año para evaluar eficacia y alineación estratégica.

20.4.5 Las acciones correctivas y preventivas deberán implementarse de manera oportuna y verificarse mediante seguimiento formal.

20.4.6 Las mejoras en sistemas de IA deberán cumplir con los principios de ética, seguridad, transparencia, protección de datos y supervisión humana.

20.4.7 Los cambios significativos en modelos de IA deberán someterse a evaluación de riesgo y revisión técnica antes de su liberación.

20.4.8 SOLTEG fomentará la cultura de mejora continua en todos los niveles, promoviendo la innovación responsable y la retroalimentación constructiva.

20.4.9 Los proveedores deberán colaborar en la implementación de mejoras cuando estas impacten servicios o componentes bajo su responsabilidad.

21. Política de Equidad, No Discriminación y Mitigación de Sesgos

SOLTEG se compromete a garantizar que todos los sistemas de Inteligencia Artificial (IA) se diseñen, desarrollen, operen y evalúen bajo principios de equidad, inclusión y no discriminación, asegurando que no generen ni amplifiquen sesgos injustos que afecten a personas, grupos o procesos institucionales. Esta política establece los lineamientos para identificar, evaluar, controlar y mitigar sesgos en datos, modelos y resultados de IA, promoviendo prácticas responsables, transparentes y alineadas con la normativa y los valores institucionales.

21.1 Objetivo

Establecer los principios y lineamientos para prevenir, detectar y mitigar sesgos en sistemas de IA, asegurando que sus resultados sean justos, imparciales y coherentes con los derechos humanos, la legislación aplicable y los objetivos institucionales; así como promover mecanismos técnicos, metodológicos y organizacionales que garanticen un uso ético y equitativo de la IA en todos los procesos donde se implemente.

GRIJALVA TECNOLOGÍA

21.2 Alcance

Esta política aplica a todos los sistemas de IA desarrollados, adquiridos, operados o supervisados por SOLTEG, incluyendo modelos internos, soluciones de terceros, servicios en la nube, APIs, datasets utilizados para entrenamiento, validación o pruebas, así como a todas las áreas, roles y proveedores que participen en el diseño, operación, evaluación o supervisión de estos sistemas.

21.3 Responsabilidades

21.3.1 Líder de Órgano Interno de Control

- Establecer lineamientos para detección, evaluación y mitigación de sesgos en datos y modelos.
- Supervisar el cumplimiento de esta política y reportar desviaciones o riesgos emergentes.
- Autorizar medidas de corrección cuando se identifiquen sesgos significativos o impactos discriminatorios.

21.3.2 Propietarios del Sistema de IA

- Evaluar el riesgo de sesgos desde la fase de diseño y documentar los resultados.
- Implementar controles de mitigación adecuados, incluyendo métricas, pruebas y revisiones periódicas.
- Validar que los outputs del sistema no generen impactos discriminatorios antes de su uso operativo.

21.3.3 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Garantizar la calidad, representatividad y balance de los datasets utilizados.
- Implementar técnicas de preprocesamiento y de fairness para reducir sesgos.
- Documentar orígenes de datos, transformaciones y limitaciones asociadas.

21.3.4 Usuarios Operativos

- Reportar resultados anómalos, inconsistentes o que puedan representar discriminación.
- Validar outputs sensibles siguiendo protocolos establecidos.
- Abstenerse de utilizar resultados sin revisión cuando existan riesgos de impacto diferenciado.

21.3.5 Proveedores y Terceros

- Proporcionar evidencia técnica sobre controles de sesgo aplicados a sus modelos o datasets.
- Cumplir con las obligaciones contractuales relacionadas con equidad y no discriminación.
- Notificar a SOLTEG sobre cualquier riesgo relacionado con bias identificado en sus herramientas.

GRIJALVA TECNOLOGÍA

21.4 Generalidades

21.4.1 Todos los sistemas de IA deberán someterse a evaluaciones de sesgo en etapas clave: diseño, entrenamiento, validación, despliegue y operación.

21.4.2 Los datasets deberán evaluarse para identificar representatividad insuficiente, desbalance o atributos sensibles no controlados.

21.4.3 Los modelos de IA deberán incluir métricas de fairness adecuadas según su tipo, contexto y nivel de riesgo.

21.4.4 Cuando se detecte sesgo significativo, se deberán aplicar acciones correctivas antes de permitir el uso del sistema.

21.4.5 Cualquier caso de potencial discriminación deberá registrarse como incidente de IA y gestionarse conforme los procedimientos del SGIA.

21.4.6 Todo el personal involucrado deberá recibir capacitación sobre sesgos, impactos y buenas prácticas de equidad en IA.

21.4.7 SOLTEG promoverá una cultura de responsabilidad y ética, evitando decisiones automatizadas que afecten derechos sin validación humana.

21.4.8 Esta política será revisada periódicamente para garantizar su vigencia y eficacia ante nuevos riesgos, modelos o tecnologías.

22. Política de Ética para el Uso Responsable de IA

SOLTEG establece esta política para asegurar que el desarrollo, uso y operación de los sistemas de inteligencia artificial se realicen bajo principios éticos, respetando la dignidad humana, la transparencia, la responsabilidad y el beneficio social, evitando cualquier daño o impacto indebido.

22.1 Objetivo

Establecer los lineamientos éticos que deben guiar todas las actividades relacionadas con la IA, garantizando decisiones responsables, protección de derechos, supervisión humana

significativa y mitigación de riesgos éticos en todo el ciclo de vida de los sistemas.

22.2 Alcance

Aplica a todas las áreas, procesos, colaboradores, proveedores, sistemas, modelos, proyectos y herramientas de IA utilizados o desarrollados por SOLTEG, incluyendo componentes internos, externos y de terceros.

22.3 Responsabilidades

22.3.1 Líder de Órgano Interno de Control
Supervisar la aplicación de los principios éticos, asegurar la gestión adecuada de riesgos y validar el cumplimiento de esta política en todos los proyectos de IA.

22.3.2 El SMT es responsable de revisar casos críticos, aprobar criterios éticos, evaluar impactos potenciales y atender situaciones que puedan comprometer la integridad o el trato justo hacia las personas.

22.3.3 Propietarios de Proceso y Dueños de Modelo de IA
Aplicar los lineamientos éticos en diseño, desarrollo, operación y mantenimiento de los modelos, asegurando supervisión humana y mitigación de sesgos.

22.3.4 Usuarios y Operadores de Sistemas de IA
Usar las herramientas de IA conforme a esta política, reportar comportamientos anómalos y evitar cualquier uso indebido, riesgoso o no autorizado.

22.4 Generalidades

22.4.1 Los sistemas de IA deben cumplir principios de transparencia, explicabilidad, equidad, no discriminación y beneficio social.

22.4.2 Toda decisión automatizada relevante debe conservar supervisión humana significativa.

22.4.3 Se prohíbe el diseño o uso de IA para fines que generen discriminación, manipulación indebida, vulneración de derechos o daño a personas o grupos.

22.4.4 Se deben identificar, evaluar y mitigar los riesgos éticos en cada fase del ciclo de vida

de los modelos.

22.4.5 El personal involucrado debe recibir capacitación continua en ética, sesgos y responsabilidad en IA.

23. Política de Validación y Verificación de Modelos de IA

SOLTEG establece esta política para asegurar que todos los modelos y sistemas de inteligencia artificial sean evaluados rigurosamente antes, durante y después de su implementación, garantizando que funcionen de manera correcta, segura, confiable y alineada con los requisitos técnicos, éticos, legales y operativos establecidos por el SGIA.

23.1 Objetivo

Definir los lineamientos para la validación, verificación y pruebas sistemáticas de los modelos de IA, con el fin de garantizar su desempeño, precisión, robustez, seguridad, trazabilidad y adecuación al propósito para el cual fueron desarrollados o adquiridos.

23.2 Alcance

Aplica a todos los sistemas, modelos, algoritmos, componentes, procesos, herramientas, proveedores y equipos internos involucrados en el diseño, construcción, entrenamiento, integración, puesta en marcha, actualización y operación de sistemas de IA dentro de SOLTEG.

23.3 Responsabilidades

23.3.1 Líder de Órgano Interno de Control

Supervisar que los procesos de validación y verificación cumplan la normatividad, los procedimientos internos y los criterios necesarios para asegurar la confiabilidad del modelo.

23.3.2 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA.

Ejecutar pruebas de validación funcional, precisión, rendimiento, robustez, seguridad y sesgos; documentar resultados y asegurar que el modelo cumpla con los requisitos definidos.

23.3.3 Propietarios de Proceso / Dueños de Modelo
Asegurar que los modelos satisfagan los requerimientos del negocio, operen dentro de límites seguros y cumplan con los criterios de aceptación antes de pasar a producción.

23.3.4 SMT
Revisar que la validación sea completa, aprobar modelos críticos y decidir si un sistema puede ser implementado o requiere mejoras adicionales.

23.3.5 Usuarios Operadores
Reportar comportamientos inesperados, degradación del desempeño o cualquier desviación detectada durante el uso cotidiano del sistema.

23.4 Generalidades

23.4.1 Todo modelo debe pasar un proceso documentado de verificación (¿se construyó correctamente?) y validación (¿resuelve correctamente el problema?).

23.4.2 La validación debe incluir monitoreo de desempeño, pruebas de sesgos, pruebas de seguridad y análisis de estabilidad ante datos extremos o adversariales.

23.4.3 Ningún modelo podrá ser implementado sin cumplir los criterios mínimos de aceptación definidos por el SGIA.

23.4.4 Todas las pruebas, resultados, evaluaciones y decisiones deben ser documentadas para garantizar trazabilidad.

23.4.5 Los modelos en producción deben someterse a revalidación periódica y validación extraordinaria ante cambios de datos, contexto o desempeño.

23.4.6 La verificación técnica debe considerar tanto código, configuración, hiperparámetros, datasets, versión del modelo y condiciones de operación.
23.4.7 Se deben utilizar métricas claras, reproducibles y consistentes para evaluar desempeño, riesgo y confiabilidad del modelo.

24. Política de Documentación y Trazabilidad del SGIA

SOLTEG establece esta política para asegurar que todos los sistemas de inteligencia artificial cuenten con documentación completa, actualizada y verificable, permitiendo la trazabilidad de decisiones, cambios, versiones, datos, modelos y procesos en todas las etapas del ciclo de vida del SGIA. Esta práctica garantiza transparencia, auditoría efectiva y control

adecuado sobre el desarrollo, operación y mejora continua de la IA.

24.1 Objetivo

Asegurar que toda la información relacionada con los sistemas de IA —incluyendo datos, modelos, algoritmos, procesos, decisiones y evidencias— sea documentada, organizada, preservada y trazable, facilitando el cumplimiento normativo, la transparencia y la reproducibilidad técnica.

24.2 Alcance

Aplica a todos los sistemas de IA, modelos, herramientas, repositorios, proveedores, procesos, personas y áreas involucradas en el diseño, entrenamiento, validación, implementación, monitoreo, mantenimiento, actualización, retiro y supervisión del SGIA.

24.3 Responsabilidades

24.3.1 Líder de Órgano Interno de Control

Definir los lineamientos de documentación, mantener el repositorio maestro del SGIA y asegurar que la información esté accesible y actualizada.

24.3.2 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

Registrar datasets utilizados, versiones de modelos, parámetros, código fuente, artefactos, bitácoras y justificaciones técnicas durante el ciclo de vida del modelo.

24.3.3 Propietarios de Proceso / Dueños de Modelo

Mantener la documentación funcional, operativa y de negocio asociada al sistema de IA, así como la descripción de requisitos, límites y casos de uso.

24.3.4 SMT

Revisar y aprobar que la documentación sea suficiente, consistente y cumpla con los controles establecidos para trazabilidad.

24.3.5 Usuarios Operadores

Reportar incidencias, anomalías y evidencias operativas que deban integrarse en los registros del SGIA.

GRIJALVA TECNOLOGÍA

24.4 Generalidades

24.4.1 Toda la documentación del SGIA debe almacenarse en repositorios seguros, con control de acceso, respaldo y versiones.

24.4.2 Se debe asegurar trazabilidad total del ciclo de vida del modelo: datos → entrenamiento → validación → despliegue → operación → retiro.

24.4.3 Cada modelo debe contar con un expediente técnico que incluya datasets utilizados, métricas, decisiones, validaciones, riesgos, aprobaciones y versiones.

24.4.4 Las decisiones clave sobre diseño, cambios, riesgos y resultados deben registrarse con evidencia verificable.

24.4.5 La documentación debe mantenerse actualizada y reflejar fielmente el estado real de cada sistema de IA.

24.4.6 La trazabilidad incluye también reclamos, incidentes, fallas, ajustes, auditorías y mejoras implementadas.

24.4.7 Toda evidencia generada debe ser conservada conforme a los tiempos definidos por los requisitos legales, normativos o internos de SOLTEG.

25. Política de Control de Cambios para Sistemas de IA

SOLTEG establece esta política para asegurar que cualquier modificación realizada en los sistemas de inteligencia artificial —incluyendo modelos, datos, infraestructura, parámetros, componentes, algoritmos, repositorios y configuraciones— sea gestionada de manera controlada, documentada y autorizada. Esto garantiza estabilidad operativa, continuidad del servicio, reducción de riesgos y cumplimiento con el SGIA.

25.1 Objetivo

Asegurar que todos los cambios en los sistemas de IA se planifiquen, evalúen, aprueben, documenten, prueben y verifiquen antes de su implementación, reduciendo riesgos operativos, técnicos, éticos y de cumplimiento.

GRIJALVA TECNOLOGÍA

25.2 Alcance

Aplica a cualquier modificación realizada en modelos, datasets, pipelines, código, infraestructura, herramientas, APIs, repositorios, proveedores, configuraciones, parámetros de entrenamiento, retraining, versiones, entornos de despliegue y cualquier elemento asociado al ciclo de vida de los sistemas de IA.

25.3 Responsabilidades

25.3.1 Líder de Órgano Interno de Control
Definir los lineamientos del control de cambios, aprobar cambios críticos y garantizar que se mantenga evidencia y trazabilidad en el SGIA.

25.3.2 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA
Registrar solicitudes de cambio, evaluar impactos técnicos, realizar pruebas, actualizar documentación y garantizar que los cambios cumplen con los criterios del SGIA.

25.3.3 Propietarios de Proceso / Dueños del Modelo
Evaluar el impacto de los cambios en el negocio, validar requerimientos, aprobar cambios no técnicos y revisar que el modelo siga cumpliendo su propósito.

25.3.4 SMT
Aprobar los cambios de alto riesgo, evaluar si requieren análisis ético, AIA, revisión de sesgos o validación adicional.

25.3.5 Usuarios Operadores
Reportar necesidades de cambio y validar que los ajustes implementados funcionan correctamente en operación.

25.4 Generalidades

25.4.1 Todo cambio debe registrarse en un sistema formal (ticket, repositorio, acta, bitácora o formulario del SGIA).

25.4.2 Se clasifican cambios como: menores, mayores y críticos, dependiendo del riesgo e impacto en resultados de IA.

25.4.3 Ningún cambio puede aplicarse sin la aprobación previa según su clasificación.

25.4.4 Deben realizarse pruebas controladas y documentadas antes del despliegue en ambiente operativo.

25.4.5 Los cambios deben incluir control de versiones, rollback plan y verificación posterior a la implementación.

25.4.6 Todo cambio debe actualizar el expediente técnico y la documentación del sistema de IA.

25.4.7 Los cambios que modifiquen comportamiento, sesgos, seguridad o métricas clave deben someterse a nueva validación y verificación.

25.4.8 Debe conservarse evidencia completa de solicitud → evaluación → autorización → pruebas → implementación → verificación.

25.4.9 Los cambios deben cumplir con requisitos legales, éticos, normativos, de seguridad y del SGIA.

26. Política de Roles y Responsabilidades del SGIA

Esta política define de manera clara y formal las funciones, atribuciones y obligaciones de los distintos actores involucrados en el Sistema de Gestión de Inteligencia Artificial (SGIA). Su objetivo es asegurar una gobernanza efectiva, evitar duplicidad o ausencia de responsabilidades y garantizar que cada sistema de IA cuente con supervisión técnica, ética, operativa y directiva adecuada.

26.1 Objetivo

Establecer y documentar los roles, responsabilidades y niveles de autoridad dentro del SGIA, asegurando una gestión organizada, responsable y alineada con los requisitos de ISO/IEC 42001, así como con las necesidades operativas de SOLTEG.

26.2 Alcance

Aplica a todas las personas que participan en el diseño, desarrollo, adquisición, operación, mantenimiento, supervisión, monitoreo, validación, administración de datos y toma de decisiones relacionadas con sistemas de IA dentro de SOLTEG, incluidos proveedores y terceros relevantes.

GRIJALVA TECNOLOGÍA

26.3 Responsabilidades

26.3.1 Director General — Dirección del SGIA

- Establecer la visión, compromiso y dirección estratégica del SGIA.
- Aprobar políticas, roles, recursos y planes del sistema.
- Presidir el Comité de IA Responsable.
- Asegurar que el SGIA cumpla requisitos legales, regulatorios y contractuales.
- Garantizar recursos suficientes para el SGIA.
- Revisar periódicamente el desempeño y la mejora continua del sistema.

26.3.2 Director de Administración y Finanzas — Gobernanza y Recursos

- Asegurar la disponibilidad de recursos financieros, humanos y tecnológicos para el SGIA.
- Coordinar inversiones en infraestructura, software y personal especializado.
- Integrar al SGIA en la gestión financiera y de gobierno corporativo.
- Evaluar costos de riesgos vs. beneficios de los sistemas de IA.
- Supervisar el cumplimiento presupuestal del SGIA.

26.3.3 Director de Operaciones

- Ser dueño funcional de los sistemas de IA bajo su operación.
- Autorizar requerimientos, cambios y despliegues de modelos.
- Asegurar que los sistemas cumplan con las necesidades del negocio.
- Supervisar su operación, métricas y desempeño.
- Coordinar con Desarrollo, Infraestructura y Riesgos los requerimientos críticos.

26.3.4 Líder de Desarrollo de IA

- Diseñar, entrenar, validar y documentar modelos de IA conforme a los requisitos del SGIA.
- Garantizar la calidad técnica, ética y regulatoria de los modelos desarrollados.
- Implementar procesos de evaluación de desempeño, robustez, equidad y explicabilidad.
- Coordinar pruebas de estrés, validación cruzada y monitoreo de drift.
- Asegurar la trazabilidad de modelos, datos y versiones.
- Colaborar con Riesgos y Control para el análisis de riesgos de IA.
- Coordinar con Infraestructura la integración segura de los modelos en producción.

26.3.5 Líder de Infraestructura y Seguridad de IA

- Implementar y mantener infraestructuras seguras para el entrenamiento y operación de sistemas de IA.

- Administrar accesos, identidades y controles de seguridad técnica.
- Ejecutar controles de protección frente a ataques adversarios y manipulación de modelos.
- Asegurar la protección del entorno de datos, APIs y pipelines de IA.
- Proveer auditorías técnicas y registros de actividad para todo el ciclo de vida.
- Coordinar con Desarrollo y Operaciones las configuraciones seguras de despliegue.

26.3.6 Líder de Operación y Soporte de Sistemas de IA

- Operar, monitorear y dar mantenimiento a los sistemas de IA en producción.
- Detectar anomalías, degradación de desempeño y necesidades de reentrenamiento.
- Gestionar incidentes de IA y activar los planes de respuesta.
- Proveer reportes de monitoreo continuo al Líder de Órgano Interno de Control.
- Garantizar la disponibilidad, continuidad y estabilidad operativa de los sistemas.
- Coordinar con Soporte Técnico el escalamiento de incidentes.

26.3.7 Coordinador de Soporte Técnico — Soporte de Primer Nivel

- Atender incidencias y solicitudes iniciales relacionadas con sistemas de IA.
- Realizar diagnósticos iniciales y escalar incidentes cuando corresponda.
- Documentar casos, tiempos de respuesta y acciones realizadas.
- Mantener comunicación con Operación y usuarios finales.
- Apoyar en monitoreos básicos y controles operativos.

26.3.8 Gerente de Compras

- Realizar evaluaciones, selección, monitoreo y reevaluación de proveedores de IA.
- Verificar el cumplimiento contractual, técnico y ético de proveedores.
- Gestionar SLAs, calidad y riesgos en cadenas de suministro de IA.
- Mantener documentación de evaluaciones de proveedores.
- Coordinar con Jurídico las cláusulas específicas de IA.

26.3.9 Gerente de Recursos Humanos

- Definir competencias, perfiles y requisitos de puestos relacionados con IA.
- Coordinar programas de capacitación y concientización del SGIA.
- Medir la eficacia de la capacitación y brechas de competencias.
- Mantener expedientes y registros de formación.
- Colaborar con líderes técnicos en programas especializados.

GRIJALVA TECNOLOGÍA

26.3.10 Coordinador de Recursos Humanos

- Operar el plan de capacitación del SGIA.
- Calendarizar cursos, convocar participantes y gestionar evaluaciones.
- Mantener registros de asistencia, evidencia y evaluaciones.
- Apoyar al Gerente de RH en la implementación de programas.
- Preparar reportes periódicos de cumplimiento de capacitación.

26.3.11 Consejería Jurídica

- Identificar y comunicar requisitos legales aplicables a los sistemas de IA.
- Revisar contratos, avisos de privacidad, licencias y obligaciones regulatorias.
- Emitir criterios legales sobre uso responsable de IA.
- Atender implicaciones de sesgos, transparencia, privacidad y responsabilidad civil.
- Asesorar en incidentes legales, regulatorios o de derechos digitales.

26.3.12 Abogada Jr.

- Dar soporte jurídico operativo al SGIA.
- Elaborar, actualizar y revisar documentos legales, contratos y anexos.
- Apoyar el seguimiento de cambios legislativos en IA, datos y tecnología.
- Preparar reportes y evidencias legales para auditorías.
- Ejecutar tareas de cumplimiento bajo la supervisión del Consejero Jurídico.

26.3.13 Líder de Riesgos y Control del SGIA

- Dirigir la identificación, análisis, valoración y tratamiento de riesgos de IA.
- Supervisar controles de supervisión humana y mecanismos de intervención.
- Mantener el registro de riesgos y reportar a la Dirección del SGIA.
- Evaluar riesgos de modelos, datos, uso indebido y fallas operativas.
- Verificar la eficacia de controles técnicos, humanos y administrativos.
- Emitir criterios para clasificación de sistemas de IA por riesgo e impacto.

26.3.14 Líder de Calidad y Cumplimiento del SGIA

- Implementar, mantener y mejorar el Sistema de Gestión de IA (SGIA).
- Supervisar el cumplimiento de políticas, controles y documentación requerida.
- Coordinar auditorías internas y la preparación para auditorías externas.
- Gestionar no conformidades, acciones correctivas y seguimiento.
- Asegurar la actualización del contexto, partes interesadas y requisitos.
- Dirigir la revisión por la Dirección del SGIA.

26.3.15 Auditor

- Planear y ejecutar auditorías internas del SGIA conforme a ISO/IEC 42001.
- Evaluar el cumplimiento de políticas, controles, roles y procesos.
- Identificar no conformidades, observaciones y oportunidades de mejora.
- Verificar la eficacia de acciones correctivas.
- Reportar hallazgos a la Dirección del SGIA y Comité de IA Responsable.

26.4 Generalidades

26.4.1 Todos los roles deberán estar formalmente designados y documentados dentro del SGIA.

26.4.2 Cada persona deberá contar con competencias demostradas para desempeñar sus funciones.

26.4.3 Las responsabilidades deberán revisarse y actualizarse al menos una vez por año.

26.4.4 Un mismo individuo podrá desempeñar varios roles solo si no existe conflicto de interés.

26.4.5 Toda delegación de autoridad deberá registrarse y mantenerse trazable.

26.4.6 El SGIA deberá garantizar continuidad en los roles críticos mediante suplencias.

26.4.7 Los roles deben alinearse con la clasificación del sistema de IA y su nivel de riesgo.

26.4.8 Las responsabilidades deben comunicarse formalmente a todo el personal involucrado.

26.4.9 SOLTEG fomentará un ambiente de transparencia, participación y responsabilidad compartida en el uso y operación de IA.

27. Política de Evaluación de Impacto (AIA)

SOLTEG reconoce que ciertos sistemas de Inteligencia Artificial pueden generar impactos significativos en personas, procesos, decisiones, datos y riesgos operativos. Por ello, esta política establece los lineamientos para realizar Evaluaciones de Impacto en IA (AIA) antes del desarrollo, adquisición, despliegue o modificación relevante de cualquier sistema, asegurando que dichos impactos sean identificados, analizados y mitigados conforme a

buenas prácticas y a ISO/IEC 42001.

27.1 Objetivo

Establecer un proceso formal para la ejecución de Evaluaciones de Impacto en IA (AIA), con el fin de identificar riesgos éticos, técnicos, legales, operativos y de seguridad antes de implementar o modificar sistemas de IA, asegurando decisiones informadas y controles adecuados.

27.2 Alcance

Aplica a todos los sistemas de IA nuevos, modificados, adquiridos, entrenados o integrados por SOLTEG, especialmente aquellos clasificados como de riesgo medio o alto, o que puedan afectar derechos de personas, servicios institucionales, procesos críticos o información sensible.

27.3 Responsabilidades

27.3.1 Líder de Órgano Interno de Control

- Aprobar la metodología institucional de AIA.
- Validar y autorizar el inicio y cierre de cada evaluación.
- Supervisar la documentación, trazabilidad y resguardo de resultados.

27.3.2 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Solicitar la realización de la AIA antes de iniciar desarrollo, despliegue o cambios mayores.
- Aportar información funcional, técnica, operativa y de contexto del sistema.
- Garantizar que los riesgos identificados sean atendidos y mitigados.

27.3.3 Líder de Desarrollo de IA, Operación y Soporte de Sistemas de IA e Infraestructura y Seguridad de IA

- Identificar riesgos técnicos, sesgos, vulnerabilidades y dependencias.
- Realizar pruebas, análisis de impacto y documentación requerida.
- Asegurar que la arquitectura soporte los controles definidos durante la AIA.

27.3.4 Área Jurídica

- Evaluar riesgos legales, regulatorios y de privacidad.
- Determinar obligaciones normativas y cláusulas contractuales necesarias.
- Validar que el sistema no contravenga limitaciones legales o éticas.

27.3.5 SMT

- Revisar evaluaciones para sistemas de riesgo medio o alto.
- Aprobar o rechazar el avance del sistema según los resultados de la AIA.
- Solicitar controles adicionales cuando existan dudas razonables.

27.3.6 Proveedores y Terceros

- Proveer documentación técnica, modelos de riesgo y evidencia de pruebas.
- Facilitar información sobre datasets, modelos y componentes externos.
- Cumplir los requisitos de la AIA definidos por SOLTEG.

27.4 Generalidades

27.4.1 Toda AIA deberá realizarse antes de desarrollar, implementar o actualizar sistemas de IA que puedan modificar su nivel de riesgo.

27.4.2 La AIA incluirá análisis de impacto ético, legal, operacional, técnico, social, de seguridad y de datos.

27.4.3 Para sistemas de alto riesgo, la AIA será obligatoria y deberá incluir revisión por el Comité de IA.

27.4.4 Los resultados deberán documentarse en un formato estándar y mantenerse trazables dentro del SGIA.

27.4.5 No se podrá desplegar ningún sistema sin que los riesgos críticos estén mitigados o aceptados formalmente.

27.4.6 Las AIA deberán revisarse periódicamente ante cambios en el sistema, en los datos o en el contexto operativo.

27.4.7 Cuando se usen servicios o modelos de terceros, la AIA deberá incluir riesgos asociados a proveedores.

27.4.8 SOLTEG garantizará que los equipos tengan la competencia necesaria para realizar estas evaluaciones.

27.4.9 Las evaluaciones deberán alinearse con principios de ética, equidad, privacidad, seguridad y transparencia.

GRIJALVA TECNOLOGÍA

28. Política de Control de Versiones, Repositorios y Artefactos de IA

SOLTEG establece esta política para garantizar el control, orden, trazabilidad y resguardo adecuado de todos los artefactos asociados al ciclo de vida de los sistemas de Inteligencia Artificial, incluyendo código, modelos, datos, configuraciones, documentación, pruebas y versiones de despliegue. Esta política asegura integridad, reproducibilidad y control sobre los cambios realizados en los componentes de IA, evitando riesgos operativos, técnicos, regulatorios o de seguridad.

28.1 Objetivo

Definir los lineamientos para gestionar versiones, repositorios y artefactos de IA con procesos estructurados de almacenamiento, control de cambios, trazabilidad y acceso seguro, garantizando que todo componente del sistema pueda ser reproducido, auditado y restaurado de manera confiable.

28.2 Alcance

Aplica a todos los artefactos generados o utilizados en el desarrollo, entrenamiento, validación, despliegue, monitoreo y mantenimiento de sistemas de IA, incluyendo datasets, código fuente, modelos entrenados, configuraciones, scripts, documentación técnica, pipelines, metadatos y registros históricos, tanto de soluciones internas como de terceros.

28.3 Responsabilidades

28.3.1 Líder de Órgano Interno de Control

- Establecer criterios y lineamientos institucionales de control de versiones.
- Garantizar la integración del proceso dentro del SGIA.
- Supervisar auditorías internas relacionadas con repositorios y artefactos.

28.3.2 Líder de Calidad y cumplimiento del SGIA

- Implementar sistemas seguros de repositorios y control de versiones.
- Registrar y versionar datasets, modelos y configuraciones.
- Mantener logs y trazabilidad completa de entrenamientos y despliegues.
- Documentar dependencias, parámetros y scripts asociados al sistema.

28.3.3 Propietarios del Sistema de IA

- Validar versiones liberadas y asegurar que cumplen con los criterios del SGIA.
- Asegurar que no existan modelos o componentes en uso sin registro formal.
- Mantener actualizada la matriz de artefactos críticos.

28.3.4 Director de Operaciones y el Líder de Infraestructura y Seguridad de IA

- Controlar accesos a repositorios según roles y principios de mínimo privilegio.
- Implementar respaldos, cifrado y políticas de retención de artefactos.
- Prevenir modificaciones no autorizadas o pérdidas de información.

28.3.5 Proveedores y Terceros

- Entregar versiones controladas y documentadas de componentes externos.
- Proveer información técnica necesaria para trazabilidad.
- Cumplir con estándares de versionamiento definidos por SOLTEG.

28.4 Generalidades

28.4.1 Todo artefacto de IA deberá almacenarse en repositorios autorizados con control de acceso.

28.4.2 Los modelos deberán versionarse indicando fecha, parámetros, dataset usado y cambios realizados.

28.4.3 Los datasets deberán tener versionado, registro de origen, anotaciones y metadatos obligatorios.

28.4.4 Queda prohibido almacenar modelos o datasets en dispositivos personales no autorizados.

28.4.5 Todo entrenamiento o reentrenamiento deberá generar un registro trazable y reproducible.

28.4.6 Deben existir respaldos automáticos y políticas de retención según criticidad.

28.4.7 Las versiones previas deberán conservarse para auditorías o restauraciones.

28.4.8 Todo cambio deberá pasar por el proceso formal de control de cambios del SGIA.

28.4.9 Los repositorios deben incluir documentación mínima obligatoria (README, dependencias, arquitectura).

28.4.10 Se deberán emplear herramientas seguras de versionamiento (Git, DVC, MLflow, etc.).

28.4.11 SOLTEG asegurará capacitación en prácticas de versionamiento y trazabilidad.

29. Política de Retiro, Descontinuación y Despliegue Seguro de Sistemas de IA

Esta política establece los criterios, procedimientos y controles para realizar el retiro, desactivación, descontinuación o reemplazo seguro de sistemas de inteligencia artificial dentro de SOLTEG. Garantiza que los sistemas obsoletos, riesgosos o no conformes se desmantelen de forma ordenada, protegida y documentada, evitando impactos operativos, de seguridad, privacidad o cumplimiento regulatorio.

29.1 Objetivo

Asegurar que el proceso de retiro y descontinuación de sistemas de IA se realice de manera segura, controlada y conforme a los principios del SGIA, garantizando la eliminación segura de modelos, datos, artefactos y configuraciones, prevención de riesgos residuales asociados a sistemas obsoletos, cumplimiento legal y normativo al finalizar su ciclo de vida y la documentación completa y trazabilidad del proceso de retiro.

29.2 Alcance

Aplica a todos los sistemas de IA desarrollados interna o externamente, modelos de aprendizaje automático, pipelines, conjuntos de datos, APIs, servicios en la nube, herramientas de análisis y cualquier componente que forme parte del ecosistema de IA de SOLTEG. Incluye sistemas en producción, pruebas, pilotos o desuso.

29.3 Responsabilidades

29.3.1 Líder del SGIA: Autorizar la descontinuación o retiro del sistema de IA y supervisar el proceso.

29.3.2 Propietario del Sistema: Solicitar el retiro, justificar la necesidad y asegurar la transferencia de conocimiento o documentación.

29.3.3 Equipo Técnico / MLOps: Ejecución del proceso de apagado seguro, eliminación de artefactos, baja de accesos y cierre de entornos.

29.3.4 Infraestructura y Seguridad de IA: Verificar la destrucción segura o anonimización de datos personales conforme a la legislación aplicable.

29.3.5 Infraestructura y Seguridad de IA: Validar que no existan vulnerabilidades o accesos residuales posteriores al retiro.

29.3.6 Auditor: Documentar el cumplimiento y verificar evidencias.

29.4 Generalidades

29.4.1 Todo retiro debe estar autorizado formalmente por el Líder del SGIA.

29.4.2 Se debe elaborar un Plan de Retiro Seguro, que incluya riesgos, pasos técnicos y controles.

29.4.3 Los modelos, datasets, versiones y artefactos deben eliminarse o archivarse según la Política de Trazabilidad y Control de Versiones.

29.4.4 Se debe garantizar la desactivación de accesos, API keys, rutas de inferencia, tokens o endpoints.

29.4.5 En caso de contener información personal, debe aplicarse la destrucción o anonimización conforme a la Política de Privacidad.

29.4.6 Los sistemas retirados deben conservar evidencia documental para auditoría durante el periodo aplicable.

29.4.7 Cualquier aprendizaje, hallazgo o mejora se documentará para mejorar futuros ciclos de vida.

29.4.8 En caso de sustitución por un nuevo modelo, se debe realizar un despliegue seguro que contemple validación previa y transferencia de parámetros.

30. Política de Balanceo y Representatividad de Datos para Sistemas de IA

SOLTEG reconoce que la calidad, representatividad y balanceo de los datos utilizados en los sistemas de Inteligencia Artificial impactan directamente en la precisión, confiabilidad, equidad, transparencia y desempeño de los modelos de IA. La presente política establece los lineamientos, controles y responsabilidades para asegurar que los datasets utilizados en actividades de entrenamiento, validación, pruebas y operación de sistemas de IA mantengan condiciones adecuadas de balance, diversidad y representatividad, reduciendo riesgos asociados a sesgos algorítmicos, discriminación, decisiones incorrectas o afectaciones operativas, en cumplimiento con los principios del Sistema de Gestión de Inteligencia Artificial (SGIA) y los requisitos de ISO/IEC 42001:2023.

30.1 Objetivo

Establecer los principios, criterios, lineamientos y controles necesarios para garantizar que los datasets utilizados en sistemas de Inteligencia Artificial mantengan niveles adecuados de balanceo, representatividad, diversidad y calidad, permitiendo reducir riesgos relacionados con sesgos, discriminación, falsos positivos, falsos negativos, pérdida de desempeño y resultados no confiables, asegurando el uso responsable, ético y seguro de los sistemas de IA de SOLTEG.

30.2 Alcance

Esta política aplica a todos los datasets utilizados en actividades relacionadas con sistemas de IA de SOLTEG, incluyendo datos de entrenamiento, validación, pruebas, reentrenamiento, monitoreo y operación continua; así como a modelos predictivos, clasificadores, modelos generativos, sistemas automatizados de decisión y cualquier solución tecnológica que incorpore Inteligencia Artificial.
Aplica también a todas las áreas, personal, proveedores, terceros, plataformas, herramientas y procesos involucrados en la recolección, preparación, limpieza, transformación, etiquetado, análisis, balanceo, validación y gestión de datos utilizados dentro del ciclo de vida de los sistemas de IA.

30.3 Responsabilidades

30.3.1. Líder de Riegos y control del SGIA

- Definir los lineamientos y criterios de balanceo de datos aplicables a los sistemas de IA.
- Aprobar metodologías, métricas y controles relacionados con representatividad y mitigación de sesgos.
- Supervisar los riesgos asociados al desbalance de datos y sus impactos potenciales.
- Asegurar que el balanceo de datos se encuentre alineado al SGIA y a los requisitos regulatorios aplicables.

GRIJALVA TECNOLOGÍA

30.3.2. Líderes de Desarrollo de IA y Operación y Soporte de Sistemas de IA

• Verificar que los datasets utilizados mantengan niveles adecuados de balance y representatividad.
• Implementar técnicas de balanceo, limpieza, validación y preparación de datos cuando sea necesario.
• Documentar las transformaciones, ajustes, técnicas y métricas utilizadas durante el balanceo de datos.
• Validar que los modelos mantengan desempeño adecuado posterior al balanceo.

30.3.3. Data Owner (Dueño del Dato)
• Garantizar que los datos utilizados sean apropiados para el propósito definido.
• Validar la representatividad y suficiencia de los datos bajo su responsabilidad.
• Autorizar el uso y transformación de datasets utilizados en IA.

30.3.4. Data Steward (Custodio del Dato)
• Mantener trazabilidad de datasets y versiones utilizadas.
• Implementar controles de almacenamiento, protección y conservación de datasets balanceados.
• Monitorear problemas relacionados con calidad, integridad o inconsistencias de datos.

30.3.5. Auditor Interno
• Verificar la existencia de controles de balanceo y validación de datasets.
• Validar la conservación de evidencia documental relacionada con análisis estadísticos, validaciones y resultados.
• Confirmar el cumplimiento de esta política durante auditorías internas del SGIA.

30.3.6. Proveedores y Terceros
• Garantizar que los datasets suministrados cumplan criterios mínimos de calidad, balance y representatividad.
• Proporcionar evidencia sobre origen, preparación y validación de datos entregados.
• Informar limitaciones, restricciones o riesgos identificados en los datasets proporcionados.

30.4 Generalidades
30.4.1. Evaluación obligatoria de datasets
Todos los datasets utilizados en sistemas de IA deberán someterse a análisis de calidad y representatividad previo a:
• Entrenamiento inicial del modelo.
• Reentrenamiento.

GRIJALVA TECNOLOGÍA

• Implementación en producción.
• Cambios significativos en el modelo.
• Incorporación de nuevas fuentes de datos.
• Actualizaciones relevantes del sistema.

30.4.2. Validación de balance y representatividad
SOLTEG deberá validar que los datasets utilizados:
• Representen adecuadamente el contexto operativo del sistema de IA.
• No presenten desbalances críticos injustificados.
• Mantengan diversidad suficiente para el caso de uso.
• Reduzcan riesgos de discriminación o sesgos indebidos.
• Sean adecuados para el objetivo funcional del sistema.

30.4.3. Técnicas de balanceo permitidas
Podrán utilizarse técnicas como:
• Oversampling.
• Undersampling.
• Balanceo híbrido.
• Ponderación estadística.
• Generación de datos sintéticos controlados.
• Técnicas avanzadas de remuestreo.
Toda técnica utilizada deberá estar documentada y justificada técnicamente.

30.4.4. Restricciones
Queda prohibido aplicar técnicas de balanceo que:
• Distorsionen artificialmente el comportamiento real del entorno operativo.
• Introduzcan datos falsos no controlados.
• Generen degradación intencional del desempeño del modelo.
• Eliminen información crítica para el análisis.
• Incumplan requisitos legales, regulatorios o contractuales.
• Vulnere derechos de privacidad o protección de datos.

30.4.5. Gestión de sesgos
SOLTEG implementará mecanismos para identificar, evaluar, reducir y monitorear sesgos asociados a:
• Datos históricos.
• Datos incompletos o insuficientes.
• Clases minoritarias.
• Variables sensibles.
• Errores de etiquetado.

• Desbalance estadístico.
• Sobre representación o subrepresentación de grupos específicos.

30.4.6. Evidencia documental obligatoria
Toda actividad relacionada con balanceo de datos deberá mantener evidencia verificable, incluyendo:
• Distribuciones estadísticas originales y finales.
• Técnicas aplicadas.
• Justificaciones técnicas.
• Resultados de validaciones.
• Métricas de desempeño.
• Riesgos identificados.
• Versiones de datasets.
• Resultados antes y después del balanceo.
• Aprobaciones correspondientes.

30.4.7. Monitoreo continuo
Los datasets y modelos deberán monitorearse periódicamente para identificar:
• Pérdida de representatividad.
• Sesgos emergentes.
• Cambios en distribución de datos.
• Degradación de desempeño.
• Incremento de falsos positivos o falsos negativos.
• Riesgos operativos o éticos asociados al modelo.

30.4.8. Integración con gestión de riesgos
Los riesgos derivados del desbalance de datos deberán integrarse al proceso de gestión de riesgos del SGIA, incluyendo:
• Riesgos éticos.
• Riesgos legales.
• Riesgos reputacionales.
• Riesgos operativos.
• Riesgos de discriminación.
• Riesgos de precisión y confiabilidad.

30.4.9. Validación y aprobación
Todo dataset balanceado deberá ser validado y aprobado antes de su uso en ambientes productivos, asegurando que:
• El desempeño del modelo sea aceptable.
• Los riesgos identificados hayan sido tratados.

• Exista trazabilidad suficiente.
• Se mantenga evidencia documental verificable.

30.4.10. Conservación de información
Toda evidencia documental relacionada con balanceo de datos deberá conservarse conforme a los lineamientos de gestión documental y retención definidos por SOLTEG y el SGIA.

30.4.11. Mejora continua
SOLTEG revisará periódicamente la efectividad de los controles de balanceo de datos mediante:
• Auditorías internas.
• Monitoreo de desempeño de modelos.
• Revisiones de calidad de datos.
• Resultados operativos.
• Hallazgos de auditoría.
• Incidentes relacionados con IA.
• Evaluaciones de impacto.

A 12 de diciembre de 2025.

Dirección General

Jesús Heriberto Hernández López Portillo