intiza

Política de Seguridad en el Uso de Inteligencia Artificial

Versión: 1.0

Confeccionó	Revisó	Aprobó
		
Carla Leiva - CISO	**Carla Leiva - CISO**	**Francisco Canale - Director**

POLÍTICA DE SEGURIDAD EN EL USO DE INTELIGENCIA ARTIFICIAL	intiza Clasificación: Restringida
Tipo: Política	Fecha vigencia: 01/10/2025
Código: PO-SI-03- Seguridad en el Uso de Inteligencia Artificial	Versión: 1.0

Contenido

1. Objetivo

El objetivo de esta política es establecer directrices claras para el uso seguro, ético y responsable de herramientas y tecnologías de inteligencia artificial (IA) dentro de la organización, garantizando la protección de la información, la propiedad intelectual, los datos personales, el cumplimiento de normativas legales y la mitigación de riesgos asociados.

2. Alcance

Esta política aplica a todos los colaboradores, contratistas, socios y terceros que utilicen herramientas de Inteligencia Artificial (IA) en actividades relacionadas con la organización, ya sea a través de plataformas internas, en la nube o servicios de terceros. Establece lineamientos de seguridad para el uso interno de tecnologías de inteligencia artificial y también para la incorporación de funcionalidades basadas en IA en los productos ofrecidos por INTIZA.

3. Responsabilidades

La totalidad de las **Áreas de la organización**, al igual que el **personal contratado**, los **proveedores** y cualquier persona que preste servicios, deberán cumplir adecuadamente con la política y sus documentos normativos dependientes.

Todo el personal de la organización, es responsable de cumplir con la presente política y sus normas relacionadas.

La **Dirección** es responsable de garantizar la implementación de esta política y asignar los recursos necesarios para su cumplimiento.

El **Comité de Seguridad** es el responsable de garantizar que la seguridad de la información se gestiona adecuadamente en las herramientas de Inteligencia Artificial homologadas por la organización.

Seguridad de la Información es responsable de definir los lineamientos de seguridad de la información relacionadas con el uso de herramientas de Inteligencia Artificial y hacer cumplir los mismos mediante una correcta gestión del SGSI.

4. Desarrollo

El uso de herramientas de Inteligencia Artificial (IA) en la organización debe cumplir con los siguientes principios:

- **Confidencialidad:** Los datos sensibles, personales o confidenciales no deben ser compartidos con herramientas de IA externas, salvo autorización explícita y tras verificar medidas de seguridad adecuadas.
- **Integridad:** Garantizar que la información procesada por la IA sea precisa y confiable.
- **Transparencia:** Comprender cómo funcionan las herramientas de IA utilizadas y asegurarse de que sus algoritmos no introduzcan sesgos o resultados discriminatorios.
- **Cumplimiento regulatorio:** Asegurar que el uso de IA cumpla con leyes y normativas aplicables, como GDPR, CCPA u otras regulaciones locales y sectoriales.

4.1. Directrices Generales para el Uso de IA

4.1.1. Gestión de Datos

- Prohibido ingresar datos sensibles, confidenciales o información personal identificable (PII) en herramientas de IA públicas sin previa autorización del área de Seguridad de la Información.

- Antes de usar una herramienta de IA, los datos deben ser anonimizados siempre que sea posible.
- Evaluar si la herramienta de IA almacena o reutiliza los datos ingresados y verificar su política de privacidad.

4.1.2. Selección de Herramientas de IA

- Solo se podrán usar herramientas de IA aprobadas por el área de TI o de Seguridad de Información.
- Las herramientas deben ser evaluadas previamente para verificar su nivel de seguridad, cumplimiento normativo y confiabilidad.
- Evitar herramientas que no ofrezcan garantías claras sobre la protección de datos o que no cumplan con los estándares de seguridad de la organización.

4.1.3. Uso Responsable

- Los usuarios deben recibir capacitación sobre los riesgos asociados al uso de herramientas de IA, incluyendo posibles brechas de seguridad, errores en los resultados y decisiones sesgadas.
- Está prohibido utilizar IA para actividades que violen las políticas internas, las leyes aplicables o los derechos de terceros.
- Toda salida generada por herramientas de IA debe ser revisada y validada antes de ser utilizada en actividades críticas para la organización. La decisión final debe recaer en un humano. La IA es una herramienta de apoyo, no de reemplazo del juicio profesional.

4.1.4. Supervisión y Auditoría

- Todas las actividades relacionadas con IA deben registrarse y ser auditables por el área de seguridad o cumplimiento, siempre que sea posible.

- El uso de herramientas de IA debe ser monitoreado periódicamente para detectar posibles incidentes de seguridad o incumplimientos.

4.2. Prohibiciones

Están prohibidas las siguientes actividades:

- Ingresar información confidencial y/o datos personales, como contraseñas, datos financieros o estrategias empresariales, en herramientas de IA públicas.
- Utilizar IA para decisiones automatizadas que puedan afectar significativamente a clientes, empleados o socios, sin supervisión humana.
- Compartir resultados generados por IA con terceros sin autorización previa.
- Utilizar IA para crear software malicioso o violar derechos de terceros.

4.3. Seguridad para el Uso Interno de IA

4.3.1. Evaluación de herramientas de IA

- Toda herramienta de IA de terceros debe ser evaluada y aprobada por el equipo de Seguridad de la Información antes de su uso.
- Se debe realizar una evaluación de riesgos, incluyendo:
    - Protección de datos proporcionados a la herramienta.
    - Ubicación de los servidores y jurisdicción legal del proveedor.
    - Cumplimiento de regulaciones aplicables.

4.3.2. Acceso y uso

- Está prohibido introducir en herramientas de IA datos sensibles de clientes, información confidencial de la empresa o propiedad intelectual sin una autorización explícita.

- Se deben proporcionar capacitaciones para asegurar que los colaboradores entiendan los riesgos asociados al uso de IA.

4.4. Seguridad para Productos con Funcionalidades de IA

4.4.1. Evaluación previa al desarrollo

- Antes de integrar IA en un producto, se debe realizar una evaluación de seguridad que incluya:
    - Identificación de riesgos asociados al modelo de IA y su impacto potencial en los clientes.
    - Evaluación de sesgos y posibles fallos que puedan generar decisiones incorrectas.
    - Análisis de privacidad y cumplimiento normativo para el tratamiento de datos del cliente.

4.4.2. Gestión de datos del cliente

- **Minimización de datos:** Solo se podrán utilizar los datos estrictamente necesarios para entrenar o ejecutar modelos de IA.
- **Consentimiento informado:** Los clientes deben otorgar autorización explícita para el uso de sus datos en funcionalidades de IA.
- **Anonimización:** Siempre que sea posible, los datos utilizados por la IA deben ser anonimizados o pseudonimizados para evitar la identificación directa de personas o entidades.

4.4.3. Evaluación de proveedores de IA

- Establecer acuerdos formales con el proveedor de IA que incluyan lineamientos de seguridad y cláusulas específicas para garantizar la protección de datos y la integridad del proceso. Estos acuerdos deben considerar:

- Acuerdo de Nivel de Servicio (SLA).
- Acuerdo de Confidencialidad (NDA) que proteja la información sensible compartida durante la colaboración.
- Cláusula de Protección de Datos. Cláusulas específicas que regulen el manejo de datos personales y sensibles, asegurando el cumplimiento de normativas vigentes.
- Derechos de Auditoría garantizando el derecho a realizar auditorías periódicas del proveedor para verificar el cumplimiento de las políticas de seguridad.
- Limitaciones de Responsabilidad definiendo claramente las responsabilidades y limitaciones de cada parte en caso de violaciones de seguridad o incumplimiento de las normativas.

- Los motores de IA externos integrados en productos (por ejemplo, OpenAI, Google AI) deben ser evaluados para garantizar:
  - Cumplimiento de estándares de seguridad y privacidad.
  - Existencia de acuerdos de nivel de servicio (SLAs) claros.
  - Protección adecuada de los datos enviados y procesados.

4.4.4. Monitoreo y auditoría

- Las funcionalidades de IA deben ser monitoreadas regularmente para detectar:
  - Sesgos o decisiones erróneas.
  - Vulnerabilidades de seguridad en los modelos.
  - Cumplimiento continuo con normativas y políticas internas.
- Se deben realizar auditorías periódicas para garantizar la seguridad y el correcto funcionamiento de los sistemas de IA.

4.4.5. Actualización y gestión de modelos

- Los modelos de IA deben ser actualizados y reentrenados únicamente por personal autorizado.
- Se debe mantener un registro de cambios y actualizaciones en los modelos.

4.4.6. Transparencia hacia los clientes

- Informar claramente a los clientes cuando se utilicen funcionalidades de IA en los productos, incluyendo:
    - Qué datos están siendo utilizados.
    - Cómo se procesan y protegen.
    - Qué decisiones o recomendaciones genera la IA.

4.5. Gestión de Incidentes Relacionados con IA

- Cualquier incidente relacionado con el uso de IA (interno o en un producto) debe ser identificado y reportado inmediatamente al equipo de Seguridad de la Información.
- Se deben tomar medidas inmediatas para mitigar el impacto del incidente, que incluyen:
    - Suspensión temporal de la funcionalidad afectada.
    - Notificación a los clientes afectados (si corresponde).
    - Investigación para identificar la causa raíz.
- Lecciones aprendidas: Incorporar los hallazgos en el proceso de mejora continua.

4.6. Cumplimiento y Sanciones

El incumplimiento de esta política puede resultar en medidas disciplinarias, que incluyen desde advertencias hasta la terminación del empleo, según la gravedad de la infracción.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Política	Seguridad de la Información	PO-SI-01
Política	Protección de Datos Personales	PO-SI-02

5.2. Definiciones y Abreviaturas

Término	Descripción
IA (Inteligencia Artificial)	Sistemas que simulan inteligencia humana para realizar tareas y que pueden mejorar a partir de datos. Se refiere a la simulación de procesos de inteligencia humana por parte de sistemas informáticos. Esto incluye el aprendizaje (adquirir información y reglas para usarla), el razonamiento (usar reglas para llegar a conclusiones), y la autocorrección. La IA abarca diversas subdisciplinas, como el aprendizaje automático, el procesamiento del lenguaje natural y la visión por computadora.
IA Privada	La **IA privada** se refiere a sistemas de inteligencia artificial que operan en entornos cerrados y restringidos, a menudo entrenados con datos confidenciales. Estos sistemas suelen ser

	propiedad de entidades específicas que desean gestionar los datos que los alimentan y conservar la propiedad intelectual de los modelos involucrados. En entornos privados de IA, la atención se centra en adaptar las aplicaciones de IA a las necesidades y objetivos específicos de la entidad propietaria. Esta personalización permite desarrollar algoritmos y modelos especializados, optimizados para los desafíos y oportunidades particulares del entorno cerrado.
IA Pública	La **IA pública** se caracteriza por su accesibilidad a un público amplio. Son sistemas desarrollados e implementados para estar ampliamente disponibles para el público o grupos específicos de usuarios. Se puede acceder a las aplicaciones públicas de IA a través de plataformas abiertas, API o servicios en la nube. Estos puntos de acceso permiten a los usuarios aprovechar las capacidades de IA sin necesidad de la extensa infraestructura ni la experiencia necesarias para ejecutar plataformas de IA privadas.
Sesgos	Un **sesgo** en inteligencia artificial (IA) se refiere a la tendencia de un modelo de IA a producir resultados que son sistemáticamente favorables o desfavorables hacia un grupo particular de personas o datos, debido a las decisiones tomadas durante el desarrollo del modelo. Este sesgo puede surgir de diversas fuentes y puede tener un impacto significativo en la equidad y la precisión de las decisiones automatizadas.

Modelos de IA	Un **modelo de inteligencia artificial (IA)** es un programa informático que ha sido entrenado para realizar tareas específicas mediante el aprendizaje a partir de datos. Este modelo utiliza algoritmos para identificar patrones y tomar decisiones basadas en la información que ha procesado.
Motores de IA	Un **motor de inteligencia artificial (IA)** es un sistema o plataforma que permite la implementación, ejecución y gestión de modelos de IA. Proporciona las herramientas y recursos necesarios para el desarrollo de aplicaciones que utilizan técnicas de inteligencia artificial, como el aprendizaje automático, el procesamiento de lenguaje natural y la visión por computadora.
Decisiones automatizadas	Las **decisiones automatizadas** son decisiones tomadas por sistemas o algoritmos sin intervención humana directa, basadas en el procesamiento de datos y modelos de inteligencia artificial.
Datos anonimizados	Los **datos anonimizados** son aquellos que han sido procesados de tal manera que ya no es posible identificar a una persona específica a partir de ellos, incluso si se utilizan métodos adicionales. Esto significa que se han eliminado o alterado todos los identificadores personales, garantizando que la información no pueda ser rastreada hasta un individuo determinado. La anonimización es irreversible, lo que implica que no se puede volver a asociar la información con la persona original.

Datos pseudoanonimizados	Los **datos pseudonimizados** son aquellos que han sido transformados de modo que la identidad de una persona ya no se puede determinar sin el uso de información adicional. En este caso, los identificadores personales han sido reemplazados por seudónimos o códigos, pero la información adicional necesaria para reidentificar a la persona se conserva de manera segura. A diferencia de la anonimización, la pseudonimización es reversible, lo que permite la reidentificación bajo condiciones controladas.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	25/09/2025	Creación de la política de Seguridad en el Uso de Inteligencia Artificial.
1.0	01/10/2025	Aprobado por Comité de Seguridad.