POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Plataforma de Generación, Ejecución y Evaluación de Exámenes con IA

Última actualización: 2 de diciembre del 2025

La presente **Política de Seguridad de la Información** establece los principios, controles y medidas que la Plataforma (en adelante, **"la Plataforma"**, **"nosotros"**, o **"el Servicio"**) implementa para proteger la confidencialidad, integridad y disponibilidad de los datos procesados, incluidos los exámenes generados y evaluados mediante inteligencia artificial (IA).

1. Objetivo de la Política

Garantizar que toda información relacionada con usuarios, docentes, estudiantes, evaluaciones, modelos de IA y procesos internos sea protegida contra accesos no autorizados, alteraciones, pérdidas, fugas o cualquier riesgo que afecte la continuidad del servicio educativo.

2. Alcance

Esta Política aplica a:

- Usuarios docentes, estudiantes y administradores
- Personal técnico y operadores autorizados
- Servidores, bases de datos y servicios en la nube relacionados
- APIs de terceros, modelos de IA externos y sistemas integrados
- Dispositivos utilizados para acceder a la Plataforma

Incluye tanto datos en tránsito como en reposo.

3. Principios de Seguridad

La Plataforma se rige por los siguientes principios:

3.1. Confidencialidad

La información sólo es accesible por personas y sistemas autorizados.

3.2. Integridad

Los datos deben mantenerse exactos, completos y sin alteraciones no autorizadas.

3.3. Disponibilidad

El sistema debe estar accesible cuando los usuarios lo requieran, salvo en ventanas de mantenimiento planificado.

3.4. Trazabilidad y Auditoría

Cada acción relevante queda registrada para fines de auditoría y detección de incidentes.

3.5. Mínimo Privilegio

Todo acceso se limita estrictamente a lo necesario según el rol del usuario.

4. Medidas Técnicas de Seguridad

4.1. Cifrado

- **Cifrado en tránsito (HTTPS/TLS 1.2+).**
- **Cifrado en reposo** mediante algoritmos seguros proporcionados por el proveedor de la nube (AES-256 o equivalente).
- Protección de claves mediante almacenamiento seguro o servicios de secreto (Vault, KMS, etc.).

4.2. Control de acceso

- Autenticación con contraseñas encriptadas (bcrypt u otro algoritmo robusto).
- Control basado en roles (RBAC) para docentes, estudiantes, administradores y sistemas.
- Bloqueo de cuentas tras intentos repetidos de acceso fallido.
- Sesiones seguras con expiración automática y protección contra secuestro de sesión.

4.3. Seguridad en API e IA

- Uso de tokens secretos y claves de API almacenadas como variables de entorno.
- Llamadas a modelos de IA con datos mínimos, anonimizados cuando sea posible.
- Validación y sanitización de entradas para evitar inyección de código o prompts maliciosos.

- Limitación de velocidad (rate limiting) para prevenir abusos o ataques automatizados.

4.4. Seguridad en servidores y nube

- Firewalls y reglas de red que restringen accesos no autorizados.
- Contenedores y microservicios aislados (Docker o equivalente).
- Actualizaciones periódicas y parches de seguridad.
- Monitoreo activo de rendimiento, latencia y anomalías.

4.5. Registro y monitoreo

- Logs de auditoría para accesos, evaluaciones y cambios críticos.
- Monitoreo de integridad y detección de comportamientos anómalos.
- Alertas automáticas ante incidentes o intentos sospechosos.

5. Medidas Organizativas

5.1. Capacitación

El personal técnico recibe formación en:

- Buenas prácticas de ciberseguridad
- Gestión de incidentes
- Manejo adecuado de datos sensibles y académicos
- Protección de datos personales (según normativa aplicable)

5.2. Gestión de incidentes

La Plataforma cuenta con un **Plan de Respuesta a Incidentes**, que incluye:

- Identificación inmediata del incidente
- Aislamiento de sistemas afectados
- Notificación a administradores o instituciones cuando sea requerido
- Documentación y análisis post-incidente

5.3. Evaluaciones y auditorías

- Revisión periódica de controles de seguridad.
- Auditorías técnicas internas o por terceros.
- Pruebas de penetración según disponibilidad.

6. Resguardo y Retención de Datos

Los datos se almacenan en infraestructuras certificadas (p. ej., ISO 27001, SOC 2 o equivalentes).
La retención se realiza conforme a la Política de Privacidad y normativas locales.

Los respaldos incluyen:

- Copias cifradas automáticas
- Mecanismos de restauración ante pérdida o daño
- Retención limitada según requerimientos institucionales

7. Transferencias Internacionales

Si los datos se procesan fuera del país del usuario:

- Se aplican cláusulas estándar de protección (GDPR u otras equivalentes).
- Los proveedores deben cumplir estándares internacionales de seguridad.

8. Seguridad en Evaluaciones y Exámenes

La Plataforma implementa medidas para preservar la integridad académica:

- Sistemas anti manipulación para preguntas y resultados
- Verificación de autenticidad del estudiante cuando la institución lo requiera
- Restricciones de navegación o supervisión remota (opcional según configuración)
- Protección contra intentos de modificar calificaciones o evaluaciones de IA

9. Responsabilidad del Usuario

Los usuarios se comprometen a:

- Mantener la confidencialidad de sus contraseñas

- Garantizar el uso adecuado del sistema según los Términos de Servicio
- No intentar vulnerar, manipular o acceder ilegalmente a funciones del sistema
- Reportar incidentes o comportamientos sospechosos

10. Actualización de la Política

Podemos actualizar esta Política de Seguridad para:

- Incorporar nuevas tecnologías
- Cumplir requisitos legales
- Mejorar controles de protección

Cualquier cambio importante será comunicado oportunamente.

11. Contacto para Seguridad

Para reportar incidentes, vulnerabilidades o riesgos:

Correo de seguridad: admin@sapiensium.com
Sitio web: www.sapiensium.com