Declaración de Aplicabilidad (SoA)

Proyecto: One Language
Versión: 1.0
Fecha: *1/10/2025*
Responsable: *Juan Pablo Gómez Perdomo y Johan Alexander Acero*

La presente Declaración de Aplicabilidad (SoA) corresponde al proyecto One Language y se ha desarrollado en conformidad con la norma ISO/IEC 27001:2022. Este documento lista los controles más críticos y aplicables del Anexo A, indicando su aplicabilidad.

ID	Control	¿Por qué es aplicable?
5.1	Políticas de seguridad de la información	Se requiere un marco formal que defina cómo proteger la información del sistema.
5.2	Roles y responsabilidades	El SRS define Administrador y Usuario; se debe asignar responsabilidades claras de seguridad.
5.3	Segregación de funciones	Para evitar que la misma persona administre y audite el sistema.
5.7	Acuerdos de confidencialidad	El equipo y proveedores deben firmar NDA para proteger la información.
5.9	Inventario de activos	El sistema maneja datos sensibles (PII, modelos ML, servidores cloud) que deben identificarse.
5.12	Clasificación de la información	Se procesan datos de distinta sensibilidad (públicos, internos, confidenciales, PII).
5.15	Control de acceso a la información	El acceso debe gestionarse según roles y privilegios mínimos.
5.17	Autenticación de la información confidencial	Las credenciales y secretos deben gestionarse de forma segura.

ID	Control	¿Por qué es aplicable?
5.23	Continuidad de la seguridad de la información	El SRS exige 99.9% disponibilidad → se requieren planes de backup y recuperación.
5.24	Gestión de incidentes	Es necesario detectar y responder a incidentes de seguridad.
5.25	Notificación de incidentes	Los usuarios deben poder reportar incidentes desde la app.
5.28	Recopilación de evidencias	Se deben conservar logs y registros para investigación de incidentes.
6.1	Selección y contratación	Si se contrata personal, debe revisarse su confiabilidad.
6.2	Términos y condiciones de empleo	Los contratos deben incluir cláusulas de seguridad.
6.3	Formación en seguridad	El equipo debe estar capacitado en seguridad y protección de datos.
6.4	Responsabilidades posteriores a la terminación	Se deben revocar accesos y recuperar activos al salir un miembro del equipo.
7.2	Seguridad de áreas de trabajo	Si se usan laptops con datos sensibles, deben protegerse físicamente.
7.9	Seguridad de equipos	Laptops y dispositivos deben tener cifrado de disco y protección física.
7.10	Almacenamiento seguro de medios	USB o discos con datos deben estar cifrados o protegidos.
8.1	Gestión de identidades y acceso	El sistema usa roles y permisos, se debe aplicar mínimo privilegio.
8.2	Autenticación de usuarios	Los usuarios acceden con credenciales, deben protegerse con contraseñas seguras y MFA en admins.

ID	Control	¿Por qué es aplicable?
8.3	Uso de información secreta de autenticación	Las contraseñas y llaves deben protegerse con hash y almacenarse de forma segura.
8.5	Principio de mínimo privilegio	Cada usuario debe tener solo los accesos necesarios.
8.6	Uso de privilegios de administración	Los administradores deben usar cuentas separadas para tareas críticas.
8.9	Registro de eventos	El SRS exige historial de sesiones → deben registrarse accesos y eventos críticos.
8.10	Monitoreo de actividades	Los logs deben revisarse para detectar anomalías.
8.11	Sincronización de relojes	Todos los servidores deben tener la hora sincronizada para coherencia en los registros.
8.12	Protección de datos en tránsito	La app transmite voz, texto y gestos → se requiere TLS/HTTPS.
8.13	Protección de datos en reposo	Los datos personales y traducciones se guardan en BD y backups cifrados.
8.14	Borrado seguro de información	Los datos de usuarios eliminados deben borrarse de forma irrecuperable.
8.15	Seguridad en desarrollo y pruebas	Los entornos de prueba deben usar datos ficticios y estar separados.
8.16	Gestión de vulnerabilidades técnicas	Se deben escanear dependencias y aplicar parches regularmente.
8.20	Seguridad del código fuente	El repositorio debe ser privado y con control de acceso.
8.21	Seguridad en servicios en la nube	Se deben evaluar proveedores cloud y establecer acuerdos de seguridad.

ID	Control	¿Por qué es aplicable?
8.23	Protección de la privacidad de la información personal	Se requiere consentimiento explícito, política de privacidad y derecho al olvido.