WAYWEB SPA

RUT 77.972.452-2 · San Joaquín · Santiago, R.M. · Chile

+56 9 6153 0165 · +56 9 6198 2297

Código: POL-SI-001

Versión: 1.0

Fecha: Mayo 2026

Clasificación: Confidencial

Páginas: 3

ANEXO A · LICITACIÓN VENTISQUEROS — PLATAFORMA TTX

Política de Seguridad de la Información

WAYWEB SPA — Versión 1.0 · Mayo 2026

CAMPO	DETALLE
Documento	Política de Seguridad de la Información
Código	POL-SI-001
Versión	1.0
Fecha de emisión	Mayo de 2026
Próxima revisión	Mayo de 2027
Propietario	Representante Legal — WAYWEB SPA
Estándar de referencia	ISO/IEC 27001:2022
Estado	Vigente

1. DECLARACIÓN DE COMPROMISO DE LA DIRECCIÓN

WAYWEB SPA, en adelante "la Empresa", reconoce que la seguridad de la información es un activo estratégico fundamental para la prestación de sus servicios y para el cumplimiento de sus obligaciones contractuales con sus clientes.

La dirección de WAYWEB SPA se compromete a:

- Establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) alineado a los principios del estándar ISO/IEC 27001:2022.
- Asignar los recursos humanos, tecnológicos y financieros necesarios para garantizar la operación segura de la plataforma SPC I.A. TTX.

- Definir y comunicar responsabilidades claras en materia de seguridad de la información a todos los colaboradores.
- Tratar la confidencialidad, integridad y disponibilidad de la información de los clientes como una obligación no negociable.

2. ALCANCE

La presente política aplica a:

- **Sistemas y plataformas:** SPC I.A. TTX y toda su infraestructura de soporte (Amazon Web Services, Google Vertex AI).
- **Personas:** Todos los colaboradores, contratistas y subcontratistas de WAYWEB SPA con acceso a sistemas o datos de clientes.
- **Datos:** Toda información de clientes, participantes de ejercicios, decisiones registradas, reportes AAR y configuraciones de la plataforma.
- **Instalaciones:** Oficinas de WAYWEB SPA y entornos de trabajo remoto utilizados para acceder a los sistemas.

3. PRINCIPIOS RECTORES

- **Confidencialidad:** La información de los clientes es accesible únicamente para personas autorizadas, con el nivel de acceso mínimo necesario para desempeñar sus funciones (principio de mínimo privilegio).
- **Integridad:** La información se protege contra modificaciones no autorizadas. Los registros de decisiones en la plataforma son inmutables por diseño (SHA-256 + ConditionExpression DynamoDB).
- **Disponibilidad:** Los servicios se mantienen disponibles según los SLA comprometidos contractualmente (99,7% anual para Plan Professional).
- **No repudio:** Cada acción relevante en la plataforma queda registrada con marca de tiempo, identidad del usuario y checksum criptográfico verificable.
- **Cumplimiento:** La operación se ajusta a la legislación chilena vigente, incluyendo la Ley 21.719 de Protección de Datos Personales.

4. CONTROL DE ACCESO

4.1 Autenticación

El acceso a la plataforma SPC I.A. TTX requiere autenticación mediante Amazon Cognito con tokens JWT firmados con algoritmo RS256. Se exige autenticación multifactor (MFA) para todos los roles administrativos.

4.2 Autorización Basada en Roles (RBAC)

El sistema implementa cinco roles con permisos granulares: Administrador, Facilitador, Participante, Observador y Evaluador. Ningún usuario puede asumir permisos superiores a los asignados a su rol. Los cambios de rol requieren autorización del Administrador de la organización.

4.3 Gestión de Credenciales

- Las contraseñas deben cumplir como mínimo: 12 caracteres, mayúsculas, minúsculas, números y símbolos.
- Las credenciales de administración de infraestructura AWS se gestionan exclusivamente mediante AWS IAM con roles asumibles, sin acceso con credenciales de larga duración.
- Las claves de API no se almacenan en repositorios de código. Se utilizan AWS Secrets Manager y Variables de Entorno cifradas.

5. CIFRADO DE DATOS

Dato en tránsito: TLS 1.3 forzado en todas las comunicaciones (API Gateway, CloudFront). HSTS habilitado. No se permite TLS 1.0 ni 1.1.

Dato en reposo: Cifrado AES-256 mediante AWS Key Management Service (KMS) con Customer Managed Keys (CMK) en DynamoDB, S3 y variables de entorno de Lambda.

Checksum de integridad: Cada decisión registrada recibe un hash SHA-256 almacenado junto al registro para verificación posterior.

6. CLASIFICACIÓN DE LA INFORMACIÓN

- **Pública:** Documentación general de la plataforma, materiales de capacitación no sensibles.
- **Interna:** Configuraciones técnicas, credenciales de entornos de desarrollo.
- **Confidencial:** Datos de clientes, registros de decisiones, escenarios de ejercicios, reportes AAR, información personal de participantes.
- **Restringida:** Claves KMS, certificados SSL/TLS, credenciales de administración de AWS.

Los datos clasificados como Confidenciales y Restringidos se almacenan cifrados, se transmiten solo bajo TLS 1.3 y se accede a ellos únicamente mediante roles autorizados con registro de auditoría.

7. GESTIÓN DE INCIDENTES DE SEGURIDAD

WAYWEB SPA mantiene un procedimiento de gestión de incidentes que contempla:

1. **Detección y notificación interna:** Todo colaborador que detecte o sospeche un incidente de seguridad debe notificarlo de inmediato al Responsable de Seguridad.
2. **Clasificación:** Los incidentes se clasifican por severidad (P1 Crítico, P2 Alto, P3 Moderado) y se activa el equipo de respuesta correspondiente.
3. **Contención:** Se toman medidas inmediatas para limitar el impacto y preservar evidencia forense.
4. **Notificación al cliente:** En caso de incidente que afecte datos de clientes, WAYWEB SPA notifica al cliente afectado dentro de las 72 horas de confirmado el incidente, conforme a la Ley 21.719.

5. **Análisis post-incidente:** Dentro de los 15 días hábiles se elabora un informe de causa raíz y se implementan medidas correctivas.

8. PROVEEDORES Y SUBCONTRATISTAS

WAYWEB SPA exige a sus proveedores con acceso a datos de clientes que cumplan con estándares equivalentes de seguridad de la información. Los principales subprocesadores son:

- **Amazon Web Services Inc.:** Infraestructura cloud. Certificado ISO/IEC 27001:2022 y SOC 2 Tipo II. Contratos de procesamiento de datos (DPA) firmados.
- **Google LLC (Vertex AI):** Procesamiento de lenguaje natural para generación de escenarios y AAR. Uso bajo Términos de Servicio Cloud con DPA.

9. RESPALDO Y CONTINUIDAD

Los datos de clientes son respaldados de forma continua mediante DynamoDB Point-in-Time Recovery (PITR), con una ventana de recuperación de 35 días y un RPO (Recovery Point Objective) de 35 segundos. El plan de continuidad completo se detalla en el Anexo C de esta propuesta.

10. REVISIÓN, AUDITORÍA Y MEJORA CONTINUA

La presente política será revisada anualmente por la dirección de WAYWEB SPA, o cuando se produzcan cambios significativos en el entorno tecnológico, legal o contractual. Adicionalmente, WAYWEB SPA se compromete a:

- Realizar una evaluación de vulnerabilidades (VA/PT) anual sobre la plataforma SPC I.A. TTX.
- Entregar a los clientes que lo requieran un resumen ejecutivo de los resultados de la evaluación de seguridad.
- Incorporar los hallazgos de auditorías y evaluaciones en el plan de mejora continua del SGSI.

11. VIGENCIA Y APROBACIÓN

La presente política entra en vigencia a partir de la fecha de firma del Representante Legal y tiene una duración de un año, renovándose automáticamente salvo revisión expresa. Cualquier excepción a esta política requiere aprobación escrita de la dirección.

APROBACIÓN Y FIRMA

Firma del Representante Legal

Mario Franjola Bustos

Representante Legal

WAYWEB SPA · RUT 77.972.452-2

Santiago, Mayo de 2026

Timbre de la empresa (si aplica)

WAYWEB SPA

San Joaquín

Santiago, Región Metropolitana

+56 9 6153 0165 · +56 9 6198 2297