Seguridad — Metodologías, Tecnologías y Comunicación

Cómo se genera, protege, transmite y consolida la información del simulador, y qué controles de seguridad respaldan cada etapa.

FECHA
6 de noviembre de 2026

CLASIFICACIÓN
Pública

VERSIÓN
1.1

Dirigido a las áreas de TI y seguridad que evalúan a Yoy como proveedor. Primero se describe la base de seguridad (infraestructura y monitoreo, secciones 01 y 02) y luego el recorrido del dato en orden: dispositivo (03), transmisión (04), acceso (05), consolidación (06) y reportes (07). Complementa a Requisitos Técnicos de Red y de Infraestructura y a Políticas Técnicas, Operativas y de Continuidad. Para el detalle de qué datos personales se tratan, con qué finalidad y por cuánto tiempo, ver la Política de Privacidad.

01. Arquitectura y seguridad de la infraestructura

Yoy Account —el backend que centraliza licencias, usuarios y reportes de uso— corre íntegramente en infraestructura cloud gestionada por Yoy.

Cómputo y datos

- Alojado en **Oracle Cloud Infrastructure (OCI)**, región Santiago de Chile
- Datos almacenados en base de datos con acceso restringido por red — sin exposición pública de esa capa
- Acceso administrativo solo por canales privados (VPN y un servicio de acceso zero-trust con identidad corporativa y doble factor), sin puertos de gestión abiertos a internet; los despliegues automatizados entran con llaves y desde una lista de IPs permitidas

Perímetro y continuidad

- Proxy, DNS y firewall gestionados por **Cloudflare**, con protección DDoS
- Certificados SSL gestionados y renovados automáticamente
- Backups automatizados mediante snapshots periódicos del servidor

02. Monitoreo y evaluación continua de seguridad

Monitoreo y escaneo continuo

- Un sistema interno de monitoreo vigila eventos de autenticación, actividad de la plataforma y el estado de la infraestructura cloud
- Alertas automáticas ante actividad anómala (ej. intentos de acceso fallidos repetidos, cambios no esperados en la configuración de red)
- Revisión periódica de la configuración de seguridad de la nube (firewall, certificados, dominios) frente a la configuración esperada

Evaluaciones de seguridad

- Revisiones internas regulares del control de acceso, la configuración de la infraestructura y las prácticas de desarrollo
- Evaluación externa (pentest) de la superficie expuesta de la plataforma, con cadencia anual; la próxima está en proceso de contratación
- Los hallazgos se priorizan y remedian, y los controles se actualizan conforme evolucionan los riesgos

03. Generación y protección de la información en el dispositivo

El simulador genera dos tipos de información durante su uso:

Resultados de evaluación

Al finalizar un ejercicio, el visor genera automáticamente un registro de resultados: puntaje global y desglose por cada parámetro evaluado.

Eventos de simulación

Durante toda la sesión, el simulador registra de forma continua lo que ocurre en la experiencia — accidentes, interacciones, manipulación de objetos, entre otros—, con sus parámetros y marca de tiempo. Yoy amplía progresivamente los eventos que capturan sus simuladores para enriquecer el análisis de desempeño.

1. **Retención transitoria en el equipo:** mientras no hay conectividad, la información se mantiene únicamente en el dispositivo, nunca como repositorio permanente del operador.
2. **Datos en reposo cifrados:** la información que queda temporalmente en el visor está cifrada.
3. **Sincronización automática:** los resultados se envían al servidor central de Yoy al finalizar cada ejercicio y los eventos, en lotes durante la sesión; el servidor pasa a ser el repositorio definitivo.

04. Comunicación segura dispositivo ↔ nube

El visor no se autentica como un usuario humano: cada dispositivo tiene credenciales de aplicación propias que validan cada solicitud contra la plataforma.

Cómo se autentica

- Cada visor se registra una sola vez con un código de un solo uso y recibe **credenciales propias**: identificador, token y clave de firma (autenticación machine-to-machine, sin intervención de un usuario)
- Cada mensaje va firmado con la clave del equipo y es de un solo uso (protección contra reenvío); las respuestas del servidor también van firmadas
- Control de acceso a nivel de **aplicación**, no de IP de origen — sin necesidad de whitelisting de IP

Qué viaja y cómo

- Único puerto saliente: **443/TCP (HTTPS)**, iniciado siempre por el dispositivo
- No se requiere abrir ningún puerto de entrada hacia la red del cliente
- Toda comunicación viaja sobre **TLS 1.2+**, sin datos sensibles en parámetros de URL
- Tres tipos de tráfico: estado de licencia (periódico), resultados de evaluación (por ejercicio) y eventos de simulación (en lotes)

Comunicación 100% saliente

No existe canal de entrada desde internet hacia la infraestructura del cliente para que el simulador funcione.

05. Control de acceso y autenticación de usuarios

Controles aplicados a la plataforma Yoy Accounts, el panel donde instructores y administradores gestionan cursos, licencias y reportes.

- **Roles estrictos por organización:** cada perfil accede solo a la información de su propia organización, sin cruce entre clientes.
- **Autenticación:** inicio de sesión con usuario/contraseña o con Google (OAuth).
- **Doble factor de autenticación (2FA):** disponible vía TOTP (aplicación autenticadora) o WebAuthn/passkeys, con recovery codes, configurable como opcional u obligatoria por organización.
- **Registro de auditoría:** los accesos y eventos relevantes del aplicativo quedan registrados para trazabilidad.
- **Cabeceras de seguridad HTTP:** HSTS, `X-Content-Type-Options` y `X-Frame-Options` aplicadas a nivel de plataforma.

06. Tratamiento y consolidación de la información

Al llegar al servidor, cada reporte se ordena automáticamente en una jerarquía que permite trazar cualquier resultado hasta su origen:

Nivel	Descripción
Organización	El reporte se asocia a la empresa cliente correspondiente.
Curso	Se ubica dentro del curso o programa de capacitación.
Unidad / experiencia	Se asocia a la unidad o ejercicio específico rendido.
Registro de evaluación	Queda el resultado global de esa evaluación.
Parámetros evaluados	Se guarda cada métrica individual que compone ese resultado (tiempo, precisión, procedimiento, etc.).

Los **eventos de simulación** se almacenan asociados al dispositivo, a la experiencia y a la actividad en que ocurrieron, lo que permite reconstruir el desarrollo de cada sesión y complementar los resultados de evaluación con el detalle de lo sucedido.

> **Acceso restringido a la base de datos**
> Todo este procesamiento vive en la base de datos central de Yoy Account, con acceso restringido por red y sin exposición pública.

07. Acceso a reportes y trazabilidad

Acceso por rol

Cada usuario entra a Yoy Accounts con el rol de su organización, sin visibilidad sobre otras empresas.

Selección de curso

Navega al curso o programa y ve el listado completo de evaluaciones rendidas.

Reporte final

Descarga el PDF individual por evaluación o exporta un Excel consolidado por curso o rango de fechas.

Adicionalmente: historial de evaluaciones por usuario y transferencia de evaluaciones entre cuentas, para corregir inscripciones cuando corresponde.

08. Contacto de seguridad y soporte

Consultas técnicas, de seguridad o reportes de incidentes:

Teléfono / WhatsApp

+56 9 7880 6021

Correo electrónico

security@yoy.cl (seguridad e incidentes)
soporte@yoy.cl (soporte)

Horario de atención: lunes a viernes, 09:00 a 18:00 (hora Chile).

Los reportes de seguridad o de vulnerabilidades enviados a **security@yoy.cl** reciben acuse de recibo dentro de **2 días hábiles** y una primera evaluación dentro de **5 días hábiles**.