Manual de administración y auditoría

Guía para auditar la consola: controles de autenticación, sesiones, autorización, integridad de la bitácora, cabeceras, infraestructura y revisión de código, con su criterio de severidad.

Manual de auditoría — Consola Abzu (demo V-2)

Versión del documento: 2026-10-16 · Consola V-2 (post-remediación) · Idioma: español

Documento para quien deba **auditar** la consola Abzu: qué verificar, dónde está cada evidencia y cómo reproducir cada control. Refleja el estado corregido tras la auditoría red-team del 2026-10-16 (4 tracks, metodología OSCP) y su remediación.

1. Mapa del sistema

Componente	Descripción	Notas
Código fuente	Repositorio del producto	Sin marcas de tecnología base en la superficie pública
Consola	Servicio web de la instalación	Acceso por HTTPS
Agente	Binario del agente en cada servidor gestionado	Canal saliente con autenticación mutua
Secretos	Almacén de secretos de la instalación, con permisos restrictivos	Nunca imprimir valores
Datos	Bitácora de auditoría y estado de la instalación	Acceso restringido
Servicios	Servicios de consola y de agente del sistema operativo	Cuentas de servicio dedicadas

El acceso para auditar se realiza con las credenciales y los procedimientos autorizados de la propia instalación.

2. Checklist de controles

2.1 Autenticación

- [ ] **Error genérico**: login con clave mala (SEGRD, gubernamental o CSRF inválido) devuelve siempre `/?error=credenciales`, sin distinguir la causa.
  - `curl -s -o /dev/null -w "%{http_code} %{redirect_url}\n" --data-urlencode "username=Ogtic" --data-urlencode "password=MALA" la ruta de inicio de sesión de la consola` (con CSRF fresco de `GET /?via=gobierno`)
- [ ] **Rate limiting**: 10 intentos / 5 min por IP → `429` + evento `login_rate_limited` en auditoría.

- [ ] **Fail-closed del proveedor de identidad**: si el proveedor SEGRD niega o falla técnicamente, NO hay fallback automático al acceso local; el error técnico muestra página 503 con link explícito a `?via=gobierno` y registra `login_proveedor_degradado`.
- [ ] **La clave nunca se persiste**: búsqueda de la palabra «password» en la bitácora → 0 coincidencias.
- [ ] **WebAuthn**: `user_verification=REQUIRED` en login (opciones de autenticación y verificación de la respuesta); detección de clon por `sign_count`; RP ID/origin por la configuración de la instalación al publicar.

2.2 Sesiones y CSRF

- [ ] Cookie `abzu_sess`: `HttpOnly`, `SameSite=Lax`, `Secure` cuando `COOKIE_SECURE=1`; helper único `_make_cookie()` (también en el flujo passkey).
- [ ] TTL 4 h + idle 60 min (`last_seen` deslizante); `tenant` ligado a la sesión y validado contra `?tenant=`.
- [ ] CSRF de un solo uso en login, logout (POST), `credentials/delete` y `register/*`; purga de expirados.
- [ ] Logout invalida en servidor: tras `POST /auth/logout`, `/api/me` → 401 con la cookie vieja.
- [ ] Sin fijación de sesión: el sid lo genera el servidor (`secrets.token_urlsafe(32)`), firmado HMAC-SHA256 con `compare_digest`.

2.3 Autorización y tenants

- [ ] Sin sesión → 401 en todos los `/api/*` (probar los 7 endpoints).
- [ ] `?tenant=<GUID-inexistente>` → 404 en `/` y `/consola`; mismatch tenant de sesión vs URL → 404.
- [ ] Lecturas sensibles (`/api/status`, `/api/backups`, `/api/audit`) dejan evento `api_read` en la bitácora.

2.4 Integridad del audit log

- [ ] Eventos registrados: `login_*_ok/fail`, `login_proveedor_degradado`, `login_rate_limited`, `login_webauthn_*`, `webauthn_register`, `logout`, `api_read`.
- [ ] El `username` se sanea (máx. 128 chars) antes de registrar; la IP se toma de la conexión salvo `TRUSTED_PROXIES` explícito (no se confía ciegamente en `X-Forwarded-For`).
- [ ] El log es append-only (`api/audit.jsonl`, 0640); verificar que ningún endpoint permite modificarlo.

2.5 Cabeceras y superficie HTTP

- [ ] `X-Frame-Options: DENY`, `Content-Security-Policy` (con `frame-ancestors 'none'`), `X-Content-Type-Options: nosniff`, `Referrer-Policy: no-referrer`; HSTS solo bajo HTTPS.
- [ ] `Server: Abzu` genérico (sin versión del entorno).

- [ ] `PUT/DELETE/PATCH/OPTIONS` → 501; `/static/../` → 404 (anti-traversal); `_read_form` topado a 256 KB → 413 si se excede.

2.6 Infraestructura

- [ ] Servicios corren como usuario de servicio dedicado (no como administrador del sistema).
- [ ] Unidades de servicio con endurecimiento: usuario dedicado, sin nuevos privilegios, sistema de archivos protegido y directorios temporales privados.
- [ ] Sin secretos en el entorno del proceso: los secretos se leen desde su almacén con permisos restrictivos y el entorno del proceso no expone nombres de secretos.
- [ ] Código y datos con propietario de servicio y permisos restrictivos; el almacén de credenciales de acceso con permiso solo para su propietario.
- [ ] Sin desviación: la huella del código desplegado coincide con la del repositorio y el árbol de trabajo está limpio.
- [ ] Configuración de privilegios sin excepciones ajenas; registros con permisos restrictivos; el diario del sistema no filtra inventario de contenedores.

2.7 Código (revisión estática)

- [ ] Sin `random` (solo `secrets`), sin invocación de intérprete de comandos ni consultas directas; `compare_digest` en comparaciones sensibles.
- [ ] `esc()` / `html.escape` en todo dato dinámico; sin `eval` / `document.write`; sin tokens en `localStorage`.
- [ ] `git log -p --all` sin secretos (solo placeholders `<redacted>` en docs).
- [ ] Agente: TLS con verificación activa; el modo sin verificación está documentado como prohibido en producción.

3. Cómo reproducir la auditoría 2026-10-16

Se ejecutó en 4 tracks paralelos (metodología OSCP, caja gris, solo lectura / explotación no destructiva):

Track	Foco	Resultado
1. Pentest web	Logins, sesiones, CSRF, tenant GUID, inyección, errores	0 críticas/altas; 3 medias (cookie Secure, RP ID por Host, CSP)
2. API	Inventario `/api/*`, autorización, integridad del audit log	2 altas (sin rate limit; fail-open del proveedor de identidad), 4 medias, 5 bajas
3. Infra/ config	systemd, permisos, secretos, red, agente	2 altas (root sin hardening; secretos en environ), 5 medias, 4 bajas
4. Code review	código de consola, interfaz y agente	2 altas (fail-open; sin user verification), 6 medias, 8 bajas

Remediación aplicada (consola V-2, desplegada y verificada): fail-closed del proveedor de identidad, rate limiting 10/5min, usuario de servicio dedicado + endurecimiento de unidades, secretos fuera del environ, `user_verification=REQUIRED`, identificador y origen de la parte confiante por configuración, cookie centralizada con `Secure`, CSRF en endpoints WebAuthn, token del proveedor en cookie HttpOnly (fuera de la URL), tope 256 KB en formularios, XFF solo desde proxies confiables, CSP + `X-Frame-Options: DENY` + HSTS, sesiones 4 h + idle 60 min + tenant ligado, purga CSRF, auditoría de lecturas API, logout por POST, texto mTLS honesto en UI.

4. Riesgos aceptados / deferidos (no son hallazgos abiertos)

- **Rebuild del binario del agente** con la cadena de herramientas actual: tarea separada en el servidor de compilación.
- **Enrollment mTLS del agente**: pendiente para v1 (hoy token estático; rotación requiere OK del dueño).
- **Rotación de credenciales del repositorio de objetos / token del agente**: recomendada como higiene, requiere autorización del responsable.
- **Actualización de la biblioteca de autenticación web**: vigilar los avisos públicos de seguridad.
- **Flujo OIDC legacy**: dormido; evaluar su eliminación.
- **Ceremonia WebAuthn completa**: pendiente de HTTPS + autenticador físico.
- **Rate limit en memoria**: se pierde al reiniciar (aceptable para demo).

5. Criterio de severidad

- **Crítica**: RCE, bypass total de autenticación, exfiltración de secretos.
- **Alta**: bypass parcial de auth, escalación, degradación silenciosa de seguridad.
- **Media**: endurecimiento necesario antes de exponer a clientes (rate limit, CSRF, headers, scoping).
- **Baja**: higiene (versiones, logs, textos, permisos no explotables hoy).

6. Frecuencia recomendada

Repetir esta auditoría (los 4 tracks) **antes de cada publicación** (`abzu.segrd.com` o actualización mayor) y tras cualquier cambio en autenticación, sesiones o WebAuthn.