Seguridad del producto

Cifrado en tránsito y en reposo, identidad y enrolamiento de agentes, sesiones, autenticación reforzada, bitácora de auditoría e informes firmados.

Alcance

Este documento resume los controles de seguridad del producto tal como constan en las fuentes públicas del expediente. Cada capacidad se etiqueta con su estado.

Cifrado en tránsito

Estado: Disponible

- El canal entre cada agente y la consola usa **TLS con autenticación mutua**: agente y consola se autentican con certificados X.509 antes de operar.
- El agente inicia siempre la conexión hacia la consola y mantiene un latido periódico firmado. No se abren puertos entrantes en los servidores gestionados por este canal y no se custodian llaves SSH centrales.

Cifrado en reposo

Estado: Disponible

- Los respaldos se cifran en flujo con **AES-256-GCM** antes de llegar a su destino.
- Las credenciales de hipervisores que custodia el agente se guardan cifradas con **AES-256-GCM**, nunca en claro.
- Los sobres del Protocolo de Custodia de Llaves se derivan con **Argon2id** y se cifran con **AES-256-GCM**.
- Los cambios sensibles registrados en la bitácora se guardan cifrados en reposo.
- En la forma gobierno, el cifrado de respaldos no es desactivable.

El inventario completo de algoritmos consta en el documento de algoritmos y módulos de esta biblioteca.

Identidad de los agentes

Estado: Disponible

- Cada agente tiene un **certificado propio**, emitido en el enrolamiento.
- El enrolamiento se realiza con un **token de un solo uso**, de vigencia breve, atado a la organización y a una etiqueta. Al usarse, el token queda consumido y no sirve una segunda vez.

- En el enrolamiento se registra además la huella del servidor, que ata la licencia a esa máquina y permite detectar duplicaciones.
- Los certificados de agente tienen vigencia limitada, se renuevan automáticamente antes de vencer y pueden revocarse; la revocación se propaga por el propio canal del agente.
- Para altas masivas existe una llave de flota reutilizable y revocable, como alternativa al token individual.

Sesiones y autenticación de usuarios

Estado: Disponible

- La consola dispone de inicio de sesión nativo en su propio dominio y, según la forma del producto, de inicio de sesión federado y de proveedores institucionales configurados por la institución.
- Las sesiones tienen duración máxima y cierre por inactividad configurables, y el cierre de sesión invalida la sesión en el servidor.
- El inicio de sesión está protegido contra intentos repetidos mediante limitación de velocidad.
- Los usuarios pueden registrar **llaves de acceso WebAuthn** (passkeys). La verificación de usuario es obligatoria en ese flujo y el sistema detecta la clonación de una llave.
- Los roles de la consola aplican denegación por defecto: operador, aprobador, auditor y solo lectura, con acciones concretas asignadas a cada rol.

Autenticación reforzada ante contexto anómalo (step-up)

Estado: Disponible

Ante un contexto anómalo —por ejemplo, una dirección de red nueva, un dispositivo nuevo o un horario inusual— la consola exige una reautenticación reforzada antes de las acciones sensibles, como destruir recetas, decidir recertificaciones o activar superficies de depuración gobernadas. Sin esa reautenticación válida, la acción sensible se deniega y la denegación queda registrada.

Bitácora de auditoría

Estado: Disponible

- Todo acto relevante queda registrado: enrolamientos, inicios de sesión, despliegues, convergencias, aprobaciones, decisiones de recuperación, cambios de licencia, recertificaciones y denegaciones de autorización, con actor, organización, momento y resultado.
- Las cadenas de registro enlazan cada entrada con la huella de la anterior; alterar o suprimir una entrada intermedia rompe la cadena y se detecta al verificarla.
- En la forma gobierno, la bitácora es local y exportable al sistema de gestión de eventos de seguridad de la institución.
- Los documentos de custodia incorporan una **marca forense documental**, cuya existencia y finalidad —atribuir filtraciones de documentos de custodia— son públicas. Su formato no se divulga.

Informes firmados

Estado: Disponible

Los informes que el producto entrega —de validación, de auditoría, de respaldos y de recuperación— se firman digitalmente con **Ed25519** mediante un módulo interno de la plataforma, sin depender de un servicio externo. Un informe sin firma registrada y verificada no se considera entregado. El procedimiento de verificación por terceros consta en el documento de informes firmados y verificación pública.

Controles adicionales declarados

Estado: Disponible

- Escaneo de imágenes en la admisión de recetas, con criterio de no actuar ante la duda: una imagen en cuarentena bloquea la aplicación.
- En la verificación de respaldos, el contenido restaurado se somete a análisis antivirus; un respaldo comprometido se marca y se aísla, y nunca se borra automáticamente.
- Separación de funciones en las operaciones críticas, incluida la recuperación ante desastres y la custodia de llaves.