Freedom · Dossier de seguridad

Documento público. Sin claves ni contraseñas. Versión 0.27.0 · generado el 2026-09-18

Qué hace Freedom para proteger los datos de las clínicas que lo usan (clientas, ventas, historias clínicas, personal) y cómo cumple con la protección de datos de Ecuador (LOPDP) y México (LFPDPPP). Escrito para leerlo sin ser informático.
Aquí no hay ninguna clave: las contraseñas y certificados viven solo en el servidor y en el gestor de contraseñas de GSL.

Versión pública: https://freedom.salon/dossier-seguridad.pdf. Dentro del programa: Manual Ø=ÜÖ !' «Seguridad». Se actualiza con cada entrega; la fecha y la versión salen al pie del PDF.

1. Quién es quién

Papel · Quién · Qué hace
Responsable del tratamiento · Cada clínica o cadena que usa Freedom (por ejemplo, HAPPYláser en Ecuador y en México) · Decide para qué se usan los datos de sus clientas y su equipo.
Encargado del tratamiento · GRUPO ESE ELE 2005, S.L. (GSL), CIF B92674621, Calle Acebuche 21, 29531 Humilladero (Málaga), España · Fabrica y aloja Freedom. Solo trata los datos siguiendo instrucciones del responsable y con contrato de encargado firmado.
Contacto de seguridad y privacidad · david@gslconsultoria.com · Incidencias, derechos de las clientas, auditorías.

2. Dónde están los datos

• Servidor principal en España (Clouding, Madrid), dentro de la Unión Europea, bajo el RGPD. Ecuador reconoce este nivel de protección para las transferencias internacionales (art. 55 y ss. LOPDP); en México la transferencia a un encargado con contrato no exige consentimiento aparte (art. 37 LFPDPPP), pero sí figura en el aviso de privacidad.
• Un servidor de reserva en otro centro de datos, con copia nocturna de la base de datos y el código listo para arrancar en menos de una hora. Cómo se activa: docs/08-plan-de-continuidad.md (versión en PDF en Ajustes !' Dirección).
• Copias: cada noche (4:30 hora de España) volcado completo de la base de datos al servidor de reserva y a Google Drive de GSL; otra copia justo antes de cada actualización del programa (se guardan las 30 últimas); prueba de restauración automática todos los domingos con aviso por correo si falla.
• Delante del programa: HTTPS obligatorio (TLS 1.2/1.3, certificado renovado solo), cortafuegos que solo abre 22/80/443, entrada por SSH únicamente con clave (nada de contraseñas), bloqueo automático de quien insiste (fail2ban) y límites de peticiones por IP en Nginx y en el programa. Los dominios apuntan directamente al servidor; poner Cloudflare como intermediario es una opción abierta (ocultaría la IP y filtraría ataques masivos), no algo que esté hecho.
• Aislamiento por organización: cada fila de cada tabla lleva su organización, su país y su centro. Toda consulta filtra por la organización del usuario; una cadena nunca puede ver ni por error datos de otra. Los datos de un país pueden vivir en un servidor propio si la ley lo pide.

3. Quién entra y cómo

• Contraseñas: mínimo 10 caracteres, se rechazan las más comunes, las repetidas, las secuencias y las que contienen el nombre o el correo de la persona. Se guardan con argon2id (no se pueden recuperar, solo cambiar).
• Doble factor (2FA) obligatorio para Dirección, Gestión y gerentes, opcional para el resto: además de la contraseña, un código de 6 cifras que genera el móvil (Google Authenticator, Microsoft Authenticator, 1Password…). Con 10 códigos de recuperación de un solo uso, guardados cifrados. Un dispositivo se puede marcar como de confianza 30 días. Dirección puede restablecer el 2FA de cualquier persona (queda registrado).
• Bloqueo por intentos: 10 fallos seguidos bloquean la cuenta 15 minutos; Dirección puede desbloquear antes.
• Sesiones: cookie que el navegador no expone (httpOnly, Secure, SameSite), caducidad configurable por la organización (12 horas por defecto, entre 1 y 72), lista de sesiones abiertas con «cerrar todas» y cierre remoto por Dirección.
• Roles: Dirección, Gestión, gerente, recepción, técnica, comercial, contable y médico; cada uno ve solo sus centros y lo

que su rol permite. Los permisos de edición sensibles (equipo, centros, ajustes, fiscal, WhatsApp) son explícitos.
• Portal de la clienta (/mi): entra con un código de un solo uso enviado a su WhatsApp; nunca ve datos clínicos por ahí, solo sus citas, bonos, pagos y documentos firmados.

4. Cómo se protege el programa

• Límites de peticiones: global (300 por minuto y dirección IP) y más estrictos en lo público y sensible: entrada (8 intentos cada 10 minutos), doble factor, portal de la clienta, formularios web, reserva online, pagos y webhooks.
• Cabeceras de seguridad (helmet): política de contenido (CSP) que solo permite código y recursos propios, sin marcos de terceros, nosniff, Referrer-Policy estricta y HSTS.
• Protección CSRF: toda petición que cambia datos con sesión tiene que venir de nuestra propia web (comprobación de Origin/Referer).
• Validación de todo lo que entra (Zod) y consultas siempre parametrizadas (sin SQL construido a mano).
• Subidas de ficheros: solo JPEG, PNG, WebP y PDF, comprobados por sus bytes reales (no por la extensión); se guardan con nombre aleatorio fuera de la web y se sirven con nosniff.
• Datos cifrados en reposo (AES-256-GCM con clave solo en el servidor): historias clínicas, fotos clínicas, medidas, certificados fiscales, tokens de WhatsApp/Meta, credenciales de pasarelas de pago, secretos del doble factor.
• Firma GSL en consentimientos, contratos y recetas: huella SHA-256 del documento antes y después, evidencias de quién, cuándo y desde dónde, sello de tiempo opcional y verificación pública por código.
• Auditoría: cada entrada, cambio, baja, acceso a una historia clínica, restablecimiento de 2FA o cambio de plan queda registrado con usuario, centro, país, IP y fecha. No se borra nada: las bajas son lógicas.
• Webhooks (WhatsApp, Meta, pasarelas de pago): solo se aceptan con firma válida del proveedor, comparada en tiempo constante; sin secreto configurado no se procesa nada.
• Secretos: nunca en el código ni en el repositorio (comprobado en todo el historial de git); en el servidor, en un fichero .env que solo lee el servicio, o cifrados en la base de datos desde Ajustes.
• Dependencias: revisadas con pnpm audit en cada entrega. Estado a 13-09-2026: 0 críticas; quedan dos actualizaciones mayores planificadas (drizzle-orm "e 0.45.2 — el aviso afecta a identificadores dinámicos, que Freedom no usa — y react-router 7).

5. Pentest interno (13-09-2026)

Se revisaron las 523 rutas del programa con un escáner propio (pnpm pentest), que comprueba que sin sesión todo responde 401/404 salvo las 47 rutas públicas y que un rol bajo (técnica) recibe 403 en todo lo de Dirección, administración, fiscal y ajustes. Además se revisaron a mano IDOR (acceder a datos de otro por el identificador), inyección SQL, XSS, CSRF, subidas de ficheros y permisos por ruta.

Encontrado y corregido en la misma entrega:

Gravedad · Qué era · Qué se hizo
Alta · Los avisos de pago de algunas pasarelas se aceptaban sin firma: con el código de un link se podía marcar una venta como pagada. · Todas las pasarelas exigen secreto configurado y firma válida; Payphone y PayPal se confirman contra su API.
Media · El secreto de los webhooks de pago lo veían roles de recepción. · Solo Gestión o quien edita Ajustes.
Media · Un documento subido a la ficha de una clienta se servía con el tipo que dijera el navegador (posible HTML malicioso). · Comprobación por bytes reales; solo imagen o PDF; nosniff.
Media · El portal de la clienta permitía adivinar si un teléfono existía. · Misma respuesta y mismo límite exista o no.
Baja · Al crear un link de pago no se comprobaba que la conversación y la clienta fueran de la misma organización. · Filtro por organización.
Baja · Parámetros láser sugeridos de una clienta accesibles por identificador y máquinas de otra organización. · Comprobación de visibilidad y organización.
Baja · Correos de newsletters y de links de pago no escapaban todo el texto; se admitían enlaces javascript:. · Escape completo y solo enlaces http(s).
Baja · Zona horaria interpolada en una consulta (ya validada). · Lista blanca estricta.
Baja · Un anónimo veía errores de validación en una ruta antes de comprobar la sesión. · Reordenado.
Baja · Contadores de límite en memoria sin purga. · Purga periódica.

Riesgos aceptados (decisión de la Dirección de GSL, revisables):
• El botón «Simular pago» de un link en modo *simulado* funciona sin sesión: es para pruebas antes de conectar la pasarela

real; en producción con pasarela real no existe.
• El canal de pruebas de WhatsApp (escribir «como clienta» desde el programa) lo puede usar cualquier persona con acceso a
Conversaciones; no sale nada a Meta.
• Los datos identificativos de las sociedades (razón social, RFC/RUC, dirección fiscal) los ve cualquier rol porque hacen
falta para vender y facturar; los certificados van cifrados en una tabla aparte.

Nota sobre el inicio de sesión: si un mismo correo existiera en dos organizaciones, el programa responde 409 y pide elegir organización en lugar de entrar en la primera que encuentre.

5b. Pentest y prueba de robustez (18-09-2026, antes del arranque)

Segunda pasada, tres días antes de salir: 661 rutas (51 públicas) con el escáner, auditoría de código y de permisos, dependencias (pnpm audit), búsqueda de secretos en el repositorio y en todo su historial, revisión del servidor y del servidor de reserva (copias, restauración, cortafuegos, SSH, TLS, cabeceras) y prueba de carga contra una copia de los datos
reales en la reserva. Sin hallazgos críticos. Encontrado y corregido en la misma noche:

Gravedad · Qué era · Qué se hizo
Alta · La IP del cliente se podía falsear con una cabecera (X-Forwarded-For), y con ello saltarse los límites por IP (login, formularios públicos) y dejar IPs falsas en la auditoría. · Nginx pasa solo la IP real de la conexión y el programa solo se fía de Nginx.
Media · El servidor de reserva admitía entrar por SSH con contraseña (un fichero de la nube ganaba a nuestra configuración). · Solo con clave, igual que el principal.
Media · La defensa CSRF dejaba pasar peticiones con Origin: null o marcadas por el navegador como de otro sitio. · Se rechazan siempre; función aparte con pruebas.
Media · El modo «producción» del programa (que apaga la entrada de desarrollo) dependía solo del fichero .env. · Fijado también en el servicio del sistema; imposible arrancar sin él.
Media · El resumen de puntos permitía pedir un centro que no era de los tuyos (misma organización). · Comprobación de centro.
Baja · El salario diario del equipo lo veían los gerentes de centro. · Solo Dirección y Gestión (RH).
Baja · Dos comparaciones de secretos (token de verificación de WhatsApp, firma de webhooks propios) no eran en tiempo constante. · timingSafeEqual.
Baja · La exportación total incluía credenciales cifradas guardadas en Ajustes. · Salen tapadas («••••••»).
Baja · Nginx anunciaba su versión; sin límites de red propios; memoria de PostgreSQL por defecto (128 MB con 8 GB de RAM); swap de 122 MB. · Versión oculta, límites por IP en Nginx, 1 GB para PostgreSQL, 2 GB de swap.
Baja · Informes de migración legibles por otros usuarios del servidor. · Permisos cerrados.
Baja · Error 500 en el contador de historias incompletas del Inicio (fechas). · Corregido.

Prueba de robustez (en el servidor de reserva, contra una copia de los datos reales: 48.000 clientas, 364.000 citas, 112.000 bonos): cuerpos de 13 MB !’ rechazados (413); JSON roto, identificadores inválidos y consultas de 100 KB !’ rechazados
(400/431); intentos de inyección SQL !’ sin efecto (todo va parametrizado); rutas con ../ !’ 403; 200 conexiones abiertas a medias durante 10 s !’ el programa sigue respondiendo en 3 ms; memoria estable (170 MB en reposo, 450 MB bajo carga).
Con 50 peticiones simultáneas la agenda responde en 0,1–0,3 s y la ficha de clienta en 0,03 s; los paneles de Inicio y Dirección (que suman todo el negocio) tardan 0,4–0,5 s cada uno y se encolan si 20 personas los abren a la vez. Se añadió un
índice para los bonos activos y se subió la memoria de PostgreSQL. El límite por IP subió de 300 a 600 peticiones/minuto
(un centro entero sale por una sola IP; el máximo real observado fue 66). Las copias de la base de datos pasan de una al día
a cuatro (04:30, 20:00, 23:00 y 02:00 hora de España), siempre también en la reserva.

Dependencias: solo tres avisos en producción (drizzle-orm, react-router), ninguno explotable con nuestro código; se actualizarán en una ventana tranquila. Ni una clave ni un dato personal en el repositorio ni en su historial.

6. Cumplimiento legal, en corto

Ecuador — Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) y su reglamento
• Datos de salud = categoría especial: se tratan con consentimiento expreso de la clienta, recogido en el consentimiento
informado firmado con Firma GSL y guardado en su expediente.
• Derechos de acceso, rectificación, eliminación, oposición y portabilidad: desde la ficha de la clienta, «Expediente completo
(PDF)» para el acceso y la portabilidad; anonimización para la eliminación cuando ya no hay obligación legal de conservar la
historia clínica (retención configurable por país en Ajustes !’ Países !’ Parámetros; por defecto 5 años).

• Registro de actividades y medidas de seguridad: este dossier y la auditoría interna del programa.
• Transferencia internacional: servidor en la Unión Europea, con nivel adecuado de protección y contrato de encargado.
• Notificación de brechas: GSL avisa al responsable en menos de 24 horas desde que la conoce para que pueda comunicarla a la
Autoridad de Protección de Datos en el plazo legal.

México — Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y NOM-004/NOM-024
• Aviso de privacidad de la clínica con consentimiento expreso para datos sensibles (salud), recogido en el consentimiento
informado con dos testigos, como pide la NOM-004 para el expediente clínico.
• Derechos ARCO (acceso, rectificación, cancelación, oposición): mismos botones del expediente; respuesta en 20 días hábiles.
• Encargado con contrato (art. 36 y 37): GSL solo trata los datos según instrucciones de la clínica; no los usa para nada más.
• Expediente clínico electrónico (NOM-024): versionado (nunca se pisa una historia), firmas con huella e integridad verificable, conservación mínima de 5 años configurable.
• Facturación (CFDI 4.0) con certificados del SAT cifrados en el servidor.

Ambos países
• Consentimiento de marketing separado (WhatsApp/correo) con baja inmediata por «BAJA»/«STOP» o enlace del correo.
• Contrato de encargado GSL !” cada sociedad de la cadena (modelo en docs/02-servidor-y-lopd.md).

7. Si pasa algo (incidentes)

1. Quien lo detecte avisa a david@gslconsultoria.com (o por WhatsApp a David) con qué ha visto y cuándo.
2. GSL contiene el problema (cerrar sesiones, bloquear cuentas, restaurar copia si hace falta) y lo anota con hora.
3. En menos de 24 horas GSL informa por escrito al responsable de qué datos y cuántas personas están afectadas.
4. El responsable decide, con el apoyo de GSL, si hay que notificar a la autoridad y a las personas afectadas.
5. Se corrige la causa y se añade al pentest para que no vuelva a pasar.

8. Lo que tiene que hacer cada clínica

• Firmar el contrato de encargado con GSL y tener publicado su aviso de privacidad / política de datos.
• Dar a cada persona su propio usuario (nunca compartidos) y darlos de baja el día que se van.
• Activar el doble factor (obligatorio para quien maneja dinero, personas o datos de salud).
• Guardar los códigos de recuperación fuera del móvil.
• Recoger el consentimiento informado antes de la primera sesión (el programa no deja dar la sesión sin él si el país lo exige).
• Revisar cada trimestre la lista de usuarios activos y las sesiones abiertas (Equipo y Ajustes !’ Seguridad).