Informe de Seguridad

Cómo protegemos tu restaurante y los datos de tu equipo

Easymanage

Publicado el 29/06/2026

Documento explicativo para clientes — versión en lenguaje claro.

Resumen para el cliente

Este documento explica, en lenguaje sencillo, las medidas de seguridad que Easymanage tiene activas hoy para proteger la información de tu restaurante: empleados, proveedores, pedidos, ventas y documentos. Para que sea fácil de entender, comparamos cada medida con prácticas habituales en aplicaciones que ya conoces (banca online, Google, WhatsApp, Apple…).

Nota: este documento describe controles que están activos en la aplicación y se actualiza cuando se añaden nuevas medidas. No constituye una certificación independiente.

Lo más importante en 30 segundos

- Cada restaurante solo ve **sus propios datos**. El servidor lo impone, no el navegador.
- Las contraseñas y los PIN de empleados **nunca se guardan en texto plano**.
- Verificación en 2 pasos (2FA) con **app de autenticación** (Google Authenticator, Authy, 1Password…).
- Todas las conexiones van **cifradas (HTTPS)**, igual que tu banca online.
- Los documentos de empleados están en un **almacén privado**; solo se abren con tu sesión.
- Los errores del servidor **no exponen detalles técnicos** a terceros.

1 · Acceso a la cuenta

El primer punto de defensa es el inicio de sesión. Aquí están las protecciones que aplicamos.

Contraseñas cifradas

Tu contraseña nunca se guarda tal cual. Se transforma en una huella matemática (hash) que no se puede revertir. Si alguien viera la base de datos, no podría leer las contraseñas. **Es la misma técnica** que usan Google, Apple o tu banco.

Verificación en 2 pasos (2FA) con app autenticadora

Activa 2FA y, además de tu contraseña, necesitarás un código de 6 dígitos de Google Authenticator, Authy o 1Password. **Mismo método** que usan GitHub, Microsoft 365, Binance o tu banco para operaciones sensibles. El código cambia cada 30 segundos y no viaja por email ni SMS (canales que pueden ser interceptados).

Sesiones gestionadas por el servidor

Cuando cierras sesión, el token deja de ser válido inmediatamente. Si pierdes el móvil o el ordenador, puedes cerrar sesión desde otro dispositivo.

2 · Aislamiento de datos entre restaurantes

Easymanage es una aplicación multi-cliente: muchos restaurantes comparten la misma infraestructura, pero **cada uno solo ve lo suyo**. Esto se llama «Row-Level Security» y lo aplica directamente la base de datos en cada consulta, no la interfaz.

Reglas de fila (RLS) en cada tabla

Empleados, proveedores, pedidos, nóminas, ingresos y gastos están protegidos por reglas que comprueban **en el servidor** que el usuario que pide los datos es el dueño. Aunque alguien manipulase la app desde el navegador, la base de datos rechazaría la consulta.

Los PIN de empleados están blindados

Los PIN se guardan cifrados (bcrypt). Además, la huella cifrada **nunca se envía al navegador**: la app solo recibe un sí/no indicando si el empleado tiene PIN configurado. Esto evita ataques de diccionario contra PINs cortos.

Documentos de empleados en almacén privado

Contratos, DNI o cualquier documento subido va a un **bucket privado**. No hay enlaces públicos. Cuando abres un documento, la app verifica en el servidor que es tuyo antes de entregarlo. Similar al funcionamiento de Google Drive o Dropbox para archivos privados.

3 · Comunicación segura

Cifrado HTTPS de extremo a extremo del navegador al servidor

Todo el tráfico entre tu navegador y Easymanage está cifrado con TLS, el mismo protocolo que usa tu **banca online** y WhatsApp Web. Nadie en la red Wi-Fi del local puede leer los datos que viajan.

Envío de pedidos a proveedores desde tu propio email

Cuando envías un pedido a un proveedor por email, se abre **tu** cliente de correo (Gmail, Outlook, Mail del iPhone) con el pedido preparado. El proveedor recibe el email desde tu cuenta real, y su respuesta te llega directamente a ti. Easymanage **no lee ni guarda** tus credenciales de correo.

4 · Funciones internas del servidor

Las funciones sensibles del servidor (consultar todas las cuentas, gestionar empleados, enviar emails internos…) están restringidas para que **no puedan llamarse** directamente desde fuera.

Funciones de administración solo para administradores

Las funciones que listan cuentas o roles comprueban internamente que quien las llama es un administrador verificado, y además están bloqueadas para visitantes anónimos.

Cola interna de emails aislada

El sistema interno que procesa emails (encolar, leer, eliminar) solo es accesible para el propio backend de confianza, nunca para usuarios o visitantes.

Errores genéricos hacia el exterior

Si algo falla, la app responde con un mensaje genérico. Los detalles técnicos (nombres de tablas, rutas internas, mensajes de la base de datos) **se guardan en logs internos** y no se exponen al usuario, como hace cualquier servicio profesional.

5 · Recuperación de PIN de empleados

Tokens de un solo uso con caducidad

Si un empleado olvida su PIN, se genera un enlace de recuperación único que caduca a la **hora**. El token se guarda hasheado (SHA-256), así que ni siquiera quien tenga acceso a la base de datos puede usarlo. Mismo patrón que Amazon o Google para resetear contraseñas.

Comparativa con apps conocidas

La siguiente tabla resume cada medida de Easymanage junto al equivalente en aplicaciones que ya usas en tu día a día. El objetivo es que veas que aplicamos las **mismas prácticas estándar** de la industria.

Medida de seguridad	Easymanage	App conocida
Contraseñas hasheadas (bcrypt)	**Sí —** Sí, nunca en texto plano	**Google / Apple:** Usan el mismo principio: jamás guardan tu contraseña tal cual.
2FA con app autenticadora (TOTP)	**Sí —** Compatible con Google Authenticator, Authy, 1Password	**GitHub / Microsoft:** Recomiendan TOTP frente a SMS por ser más seguro.
Cifrado en tránsito (HTTPS/TLS)	**Sí —** Todo el tráfico cifrado	**Banca online:** Mismo candado verde en la barra del navegador.
Aislamiento entre clientes	**Sí —** Row-Level Security a nivel de base de datos	**Slack / Notion:** Cada workspace ve solo sus propios datos.
Documentos privados	**Sí —** Bucket privado + verificación en cada apertura	**Google Drive / Dropbox:** Los archivos no son accesibles sin permiso.
PINs almacenados con bcrypt	**Sí —** Hash + nunca enviado al navegador	**Apple Pay / banca móvil:** El PIN no viaja ni se almacena en claro.
Enlaces de recuperación con caducidad	**Sí —** Token de un solo uso, caduca en 1h	**Amazon / Google:** Enlaces de reset también caducan y son de un solo uso.
Sin exposición de errores internos	**Sí —** Logs internos; al cliente, mensaje genérico	**Stripe / AWS:** Práctica estándar para no dar pistas a atacantes.
Funciones admin protegidas	**Sí —** Doble check: rol admin + acceso restringido	**Panel admin de WordPress:** Solo administradores pueden entrar al panel.

Lo que depende de ti

La seguridad es una responsabilidad compartida. Easymanage pone los controles técnicos, pero hay buenas prácticas que ayudan mucho:

- Usa una **contraseña fuerte y única** para Easymanage (no la repitas en otros sitios).
- Activa la **verificación en 2 pasos** desde Configuración → Seguridad.
- Cierra sesión en dispositivos compartidos del local.
- Avisa al equipo de no compartir su PIN personal con nadie.
- Mantén el navegador actualizado.

Contacto de seguridad

Si detectas algo inusual en tu cuenta o quieres reportar un posible problema de seguridad, escríbenos. Tratamos cada aviso con prioridad.

Email: jjnevesmanagement@gmail.com

Este informe describe controles activos a fecha de publicación. Easymanage continúa incorporando mejoras de seguridad de forma periódica.