Política de Seguridad

Versión 1.0 · Vigente desde el 04/08/2026 · Última actualización: 04/08/2026

1. Compromiso de seguridad

La seguridad de la información es un componente esencial del servicio. GearDash aplica medidas técnicas, humanas y administrativas razonables y proporcionales a la naturaleza de los datos tratados, en línea con el principio de seguridad del artículo 4 de la Ley 1581 de 2012.

Ninguna plataforma puede garantizar seguridad absoluta; el compromiso de GearDash es de diligencia: prevenir, detectar y responder a incidentes conforme a esta política.

2. Aislamiento multi-tenant

Cada taller opera en un espacio lógico aislado: todas las consultas a la base de datos se filtran automáticamente por la identidad del taller (filtros globales a nivel del motor de acceso a datos), de modo que un taller no puede ver ni alterar la información de otro.

El acceso administrativo transversal está restringido al personal autorizado de GearDash y las sesiones de soporte sobre un taller quedan identificadas de manera visible.

3. Control de acceso y autenticación

Controles principales de acceso:

- Autenticación basada en ASP.NET Core Identity, con contraseñas almacenadas mediante hash criptográfico con sal (nunca en texto plano).
- Autorización por roles (Administrador, Mecánico, SuperAdministrador) que restringe cada módulo y acción al perfil correspondiente.
- Gating por plan validado tanto en la interfaz como en el backend: las restricciones no dependen solo del navegador.
- Sesiones protegidas con cookies seguras y protección antifalsificación de solicitudes (antiforgery) en las operaciones de escritura.

4. Protección de datos en tránsito y en reposo

Medidas de protección de la información:

- Cifrado del canal mediante HTTPS/TLS para todo el tráfico entre el navegador y la plataforma.
- Credenciales de integraciones externas (API keys, tokens, contraseñas de proveedores tecnológicos) cifradas en reposo mediante ASP.NET Core Data Protection.
- La interfaz nunca reexpone secretos guardados: los campos sensibles se muestran vacíos y solo se reemplazan si el Cliente ingresa un valor nuevo.
- Validación de destinos de red en las integraciones salientes para bloquear accesos a redes privadas (mitigación de SSRF).

5. Infraestructura, respaldos y continuidad

La plataforma se aloja en infraestructura de proveedores especializados con controles físicos y lógicos propios. La base de datos cuenta con los mecanismos de respaldo del proveedor de infraestructura; adicionalmente, la plataforma implementa políticas de reintento y tolerancia a fallos transitorios de conexión.

Política de Seguridad

Versión 1.0 · Vigente desde el 04/08/2026 · Última actualización: 04/08/2026

Los mantenimientos y ventanas de actualización se gestionan conforme al SLA del Centro Legal.

6. Gestión de incidentes

Ante un incidente de seguridad, GearDash: (i) contiene y mitiga el evento; (ii) evalúa el alcance y los datos afectados; (iii) notifica a los talleres afectados con información útil y oportuna; y (iv) reporta a la Superintendencia de Industria y Comercio cuando el incidente afecte datos personales y la normatividad lo exija.

Cualquier persona puede reportar vulnerabilidades o incidentes a través de el canal de soporte habilitado dentro de la plataforma GearDash. GearDash agradece la divulgación responsable y no emprenderá acciones contra investigaciones de buena fe que respeten los datos de los clientes.

7. Responsabilidades del Cliente

La seguridad es corresponsabilidad del Cliente, quien debe:

- Custodiar sus credenciales y las de sus usuarios; usar contraseñas robustas y únicas.
- Desactivar oportunamente los usuarios de personal retirado.
- Mantener seguros los dispositivos y redes desde los que accede a la plataforma.
- Reportar de inmediato cualquier acceso sospechoso o pérdida de credenciales.

Documento publicado en https://geardash.runasp.net/legal/seguridad. Este PDF reproduce fielmente la versión indicada en el encabezado.