

Guía Ejecutiva: Protección de Datos y Seguridad

Versión: 1.4

Responsable: Dirección + Responsable Técnico

Fecha de emisión: 18 de febrero de 2026

Última revisión: 5 de mayo de 2026

Próxima revisión: 15 de diciembre de 2026

Acrónimos usados

- **PII:** Información de Identificación Personal.
- **RGPD:** Reglamento General de Protección de Datos (UE 2016/679).
- **LOPDGDD:** Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
- **LSSI-CE:** Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- **CSP:** Content Security Policy.
- **XSS:** Cross-Site Scripting.
- **CI:** Integración Continua.
- **KPI:** Key Performance Indicator.
- **pg_cron:** Extensión de PostgreSQL para programar tareas periódicas.
- **CSV:** Comma-Separated Values.

1) Mensaje clave para dirección

ADDIF tiene implantados controles críticos de protección de datos y seguridad que **reducen de forma sustancial** el riesgo legal, operativo y reputacional. Los formularios web de contacto y voluntariado están cerrados; se mantienen los registros históricos bajo controles de acceso y retención. Se mantiene **riesgo residual controlado**, con seguimiento mensual de indicadores.

2) Qué estamos protegiendo

- Datos personales de contacto.
- Datos de voluntariado.
- Datos de donación y trazabilidad administrativa.
- Accesos al panel de administración y operaciones sensibles.

3) Qué controles están activos

Gestión de secretos

- Secretos fuera de archivos versionados.
- Validación de variables críticas en producción.
- Runbook operativo para rotación y revocación.

Retención y minimización de datos

- Eliminación automática por política:
 - contacto: 12 meses
 - voluntariado: 24 meses
 - donaciones: 72 meses
- Auditoría de cada ejecución de purga.
- Ejecución diaria por pg_cron o workflow de plataforma.

Control de acceso

- Exportación de donaciones limitada a rol admin.
- Registro de auditoría de exportaciones (quién, qué, cuándo).
- Flujo administrativo interno RGPD endurecido para registrar, asignar, verificar identidad, exportar y resolver solicitudes.
- Verificación manual de identidad obligatoria antes de exportar, rectificar, suprimir o denegar solicitudes RGPD.
- Bloqueo legal de donaciones cuando no procede supresión por conservación obligatoria.

Seguridad de aplicación web

- CSP activa y monitorizada.
- Modo CSP estricto disponible para endurecimiento adicional.
- Endpoint de reportes CSP con límites, saneado y deduplicación.

Anti-abuso y disponibilidad

- Rate limit en endpoints críticos.
- Soporte de backend distribuido (Redis/Upstash) y Retry-After consistente.
- Protección específica en login ante fuerza bruta.
- Cloudflare Turnstile aplicado en login; contacto y voluntariado web están cerrados y ya no ejecutan esos flujos antiabuso.

Logging seguro

- Redacción de IP, URL, user-agent y campos sensibles.
- Política de menor exposición de datos en producción.
- Cobertura homogénea de redacción segura para los dominios con PII actualmente identificados.

Cookies y transparencia

- Operativa actual alineada a “solo cookies técnicas”.
- Documentación legal actualizada y republicada para coherencia con la operación real.

4) Riesgos mitigados (visión negocio)

- Fuga por mala gestión de credenciales: **riesgo reducido y controlado**.
- Conservación excesiva de PII: **riesgo reducido y controlado**.
- Exportaciones indebidas de donaciones: **riesgo reducido y controlado**.
- Abuso de formularios/login: **riesgo reducido y controlado**.
- Exposición de PII en logs: **riesgo reducido y controlado**, con vigilancia sobre nuevos tratamientos para evitar regresiones.

5) Evidencias que puede revisar dirección

- PR de hardening de esta fase: <https://github.com/pangeaexp/addif-web/pull/38>.
- Migración de retención CSP:
supabase/migrations/20260319_schedule_csp_reports_retention.sql.
- Migración de solicitudes RGPD y restricciones de donaciones:
supabase/migrations/20260331_add_gdpr_requests_and_donation_restrictions.sql.
- Endurecimiento operativo de solicitudes RGPD:
supabase/migrations/20260421_harden_gdpr_requests_operability.sql.
- Evidencia de tests CI en verde:
 - npm run test:ci
 - npm run lint
 - npm run build
- Tabla de auditoría de retención en BD:
 - public.security_data_retention_audit.
- Tabla de auditoría de exportación de datos personales:
 - public.personal_data_export_audit.
- Workflow de retención PII en GitHub Actions (runbook operativo).

6) Decisiones de gestión que deben mantenerse

- Mantener política de retención 12/24/72 salvo cambio legal interno.
- Revisar rotación de secretos de forma periódica.
- Mantener “solo técnicas” en cookies hasta decisión formal de analítica.
- Activar CSP estricto por ventana controlada cuando se autorice.
- Mantener revisión trimestral de proveedores y documentación legal publicada.
- Mantener la exigencia de identidad verificada antes de cualquier exportación o resolución RGPD en backoffice.

7) Indicadores ejecutivos (KPI recomendados)

- % ejecuciones retención exitosas (objetivo: 100%).
- N° accesos de exportación de donaciones por mes.
- N° exportaciones RGPD con identidad verificada frente a solicitudes registradas.
- N° resoluciones RGPD cerradas sin incidencia de verificación de identidad.
- N° bloqueos por rate limit (tendencia de abuso).
- N° incidentes de seguridad con PII (objetivo: 0).
- Edad media de secretos críticos (días desde última rotación).

8) Protocolo ante incidente (resumen)

1. Contener: revocar clave/aislar acceso.
2. Evaluar impacto: qué datos, qué periodo, qué sistemas.
3. Corregir: rotar, parchear, validar.
4. Comunicar: equipo interno, legal y partes afectadas si aplica.
5. Prevenir: acción correctiva registrada con responsable y fecha.

9) Guion de 5 minutos para comité

1. Ya cerramos fase crítica con controles activos en secretos, retención, acceso y anti-abuso.
2. El tratamiento de datos está acotado por plazos técnicos auditables (12/24/72).
3. La exportación de donaciones está restringida a admin y auditada.
4. Ya existe un flujo interno endurecido para derechos RGPD con identidad obligatoria antes de exportar o resolver y bloqueo legal de donaciones cuando la conservación prevalece.
5. La web tiene hardening activo (CSP, rate limit, Cloudflare Turnstile en superficies clave, logs redactados con cobertura homogénea en los dominios identificados, limpieza CSP programada).
6. La documentación legal y ejecutiva publicada ya está alineada con el estado operativo actual.
7. Siguiendo foco de gobernanza: consentimiento/analytics, anonimización y seguimiento mensual de KPIs.

10) Alcance y exclusiones

Alcance

- Controles técnicos y operativos de protección de datos y seguridad aplicados en la plataforma web ADDIF.
- Procesos de retención, auditoría, acceso admin y prevención de abuso en APIs.

Exclusiones

- No cubre auditorías de terceros fuera de la plataforma ADDIF.
- No cubre continuidad de negocio/DRP corporativo.

- No sustituye asesoría legal formal ni evaluaciones regulatorias específicas por caso.

11) Nota de accesibilidad documental

Esta guía debe publicarse en formato accesible (PDF etiquetado) para distribución institucional y cumplimiento de buenas prácticas de accesibilidad.