

Política de Privacidad C.O EL NIGERIANO J.J

Vigencia: inmediata

Última revisión: 23 de septiembre de 2025

Titular/Responsable: C.O EL NIGERIANO J.J (“Empresa”, “MARCA”)

Sitio: <https://coelnigerianojj.com>

Contacto privacidad: sales@coelnigerianojj.com • P.O. Box 20741, San Juan, PR 00928

1. Declaración de principios, alcance y fundamento

1.1 Compromiso y estándar. Tratamos datos personales bajo principios de licitud, lealtad y transparencia; limitación de finalidad; minimización; exactitud; limitación de conservación; integridad y confidencialidad; y responsabilidad proactiva. Este estándar deriva de normas de protección al consumidor y de privacidad aplicables en Puerto Rico/EE. UU. y de buenas prácticas internacionales (privacy by design & by default).

1.2 Ámbito material y canales. Esta Política rige el Sitio, subdominios, procesos de checkout, post-venta, helpdesk, integraciones con pasarelas de pago y logística, y cualquier formulario o interfaz habilitados por la Empresa.

1.3 No sustitución de T&C. Esta Política se integra a los Términos y Condiciones (T&C). En caso de conflicto interpretativo, prevalecerá la regla más protectora para el Usuario sin desnaturalizar obligaciones contractuales.

1.4 Quién es quién (resumen funcional).

a) Responsable: Empresa. b) Encargados: proveedores bajo contrato (hosting/CDN, pasarela de pagos, logística, anti-fraude, helpdesk). c) Terceros independientes: servicios con políticas propias cuando interactúas voluntariamente (p. ej., redes sociales).

2. Base jurídica del tratamiento (argumento)

2.1 Ejecución de contrato: imprescindible para crear cuenta, tramitar pedidos, facturar, enviar, atender RMA y garantías. Sin estos datos, la venta no es viable.

2.2 Cumplimiento de obligaciones legales: fiscales/contables, seguridad del producto, atención de reclamos, gestión de contracargos y cooperación con autoridades competentes.

2.3 Interés legítimo (balanceado y documentado): seguridad (WAF/anti-bot, logs), prevención de fraude (señales de riesgo, verificación razonable), mejora de servicio y métricas operativas (sin perfiles invasivos), continuidad de negocio.

2.4 Consentimiento: cookies/SDK no esenciales, newsletters y marketing electrónico; podrás retirar tu consentimiento en cualquier momento (sin efecto retroactivo).

2.5 Interés vital/orden público: sólo en supuestos excepcionales (p. ej., seguridad de usuarios, alertas sanitarias de producto).

3. Categorías de datos y finalidades (mapa exhaustivo)

3.1 Identificación y contacto (nombre, correo, teléfono, direcciones): registro, soporte, envíos, facturación.

3.2 Transaccionales (carrito/pedidos, importes, productos, tokens/ID de pasarela; nunca PAN completo ni CVV): cobros, reembolsos, conciliación, antifraude.

3.3 Técnicos/seguridad (logs): IP, user-agent, device ID razonable, timestamps, intentos de autenticación, MFA, cambios sensibles, eventos WAF/anti-bot/API: ciberseguridad, continuidad, cumplimiento.

3.4 Soporte/posventa: fotos/videos para reclamos, RMA, comunicaciones: verificación de incidencias y garantías.

3.5 Preferencias/marketing: opt-in/opt-out, configuración de cookies; envío de comunicaciones lícitas y medición agregada.

3.6 KYC/Verificación (B2B/alto riesgo): datos de entidad/representantes, good standing, certificados de exención/reseller: gestión de riesgo, legitimación de la relación.

3.7 No solicitamos categorías sensibles (salud, biométricos, etc.). Si el Usuario las remite por error, se eliminarán o blindarán con medidas reforzadas.

4. Origen de los datos y criterios de pertinencia

4.1 Directo (el Usuario los proporciona); automático (interacción técnica con el Sitio); derivado (pasarelas/transportistas: confirmaciones, tracking).

4.2 Pertinencia: sólo pedimos lo estrictamente necesario para la finalidad declarada. Formularios utilizan campos mínimos y validaciones básicas (ej. correo verificado).

5. Cookies/SDK y panel de consentimiento (CMP)

5.1 Categorías: estrictamente necesarias (activas por defecto), funcionales, analíticas/medición, publicidad.

5.2 Régimen de activación: las no esenciales solo se cargan con opt-in. Registramos log de consentimiento (versión, fecha/hora, preferencia).

5.3 Gestión: podrás revocar o ajustar preferencias en cualquier momento desde el panel. El detalle técnico figura en el Aviso de Cookies (parte integrante de esta Política).

5.4 Do Not Track: actualmente no respondemos a señales DNT del navegador si el estándar no es uniforme; respetamos el consentimiento del CMP.

6. Pagos: seguridad y no almacenamiento de credenciales

6.1 Procesamos pagos exclusivamente vía proveedores PCI DSS (p. ej., Stripe/PayPal/ATH Móvil Business, según se informe en el checkout).

6.2 La Empresa no almacena PAN/CVV. Conservamos tokens no sensibles para conciliación, reembolsos y gestión antifraude.

7. Encargados/terceros: contratos y salvaguardas

7.1 Todo encargado firma contrato con confidencialidad, seguridad equivalente, limitación de finalidad, control de subencargados y notificación temprana de incidentes.

7.2 En integraciones opcionales (p. ej., redes sociales, mapas), tus datos se rigen también por las políticas de dichos terceros. Recomendamos revisarlas antes de usarlos.

8. Transferencias internacionales

8.1 Sólo realizamos transferencias necesarias para la operación (p. ej., CDN global, pasarela, nube). Cuando impliquen países sin nivel “adecuado”, aplicamos cláusulas contractuales tipo u otras garantías equivalentes y una evaluación de riesgos del destino.

8.2 No transferimos datos a jurisdicciones sancionadas ni en contravención de controles de exportación.

9. Conservación y borrado (retención)

9.1 Criterio general: “solo lo necesario, por el tiempo necesario”.

- **Cuenta y perfil: relación activa + hasta 2 años (defensa de reclamaciones).**
 - **Facturación/contabilidad: 5–7 años (exigencias fiscales).**
 - **Logs de seguridad: autenticación 12 meses; eventos críticos 24 meses; incidentes: hasta cierre + plazos legales.**
 - **Marketing: mientras consentimiento o relación o hasta opt-out.**
- 9.2 Implementamos borrado seguro o anonimización al vencer los plazos, con registro de la acción.**

10. Seguridad (defensa en profundidad)

10.1 Controles técnicos/organizativos: TLS; cifrado en tránsito y, cuando aplique, en reposo; MFA en accesos sensibles; mínimo privilegio; WAF/IDS/IPS; rate-limiting/anti-bot; segregación de entornos; backups; gestión de parches; monitorización; pruebas de vulnerabilidades y, cuando proceda, pentesting.

10.2 Gestión de claves: rotación periódica, bóvedas seguras, prohibición de secretos embebidos en código.

10.3 Integridad probatoria: en incidentes de alto impacto, paquete de evidencia con sellado de tiempo, hash y cadena de custodia.

11. Antifraude y verificación razonable (KYC)

11.1 Podemos requerir verificación (e-mail/teléfono, dirección, coincidencia titular-pago, documento de identidad o corporativo) ante señales de riesgo: múltiples intentos fallidos, discrepancias de identidad/dirección, IP/TOR/ASN de riesgo, uso inusual de cupones, historial de chargebacks.

11.2 Principios: no discriminación, minimización y tratamiento conforme a esta Política.

11.3 Medidas proporcionales: solicitud de información adicional, retención temporal de pedido, cancelación con reembolso, cierre de cuenta, bloqueo de medios de pago/dispositivos irregulares.

12. Derechos del Usuario/Cliente y proceso de atención

12.1 Derechos: acceso, rectificación, actualización, supresión, oposición, limitación y portabilidad (cuando proceda).

12.2 Cómo ejercer: sales@coelnigerianojj.com o formulario del Sitio. Acuse ≤ 5 días hábiles; resolución ≤ 30 días (prorrogable por complejidad con aviso).

12.3 Verificación proporcional de identidad para proteger cuentas/datos (ej. confirmación vía correo verificado). Anti-represalias: no habrá trato desfavorable por ejercer derechos.

12.4 Marketing: opt-out inmediato desde el enlace de baja o panel de preferencias; SMS se rigen por TCPA (consentimiento expreso por escrito; “STOP” para desuscribirse).

12.5 Recurso/Apelación (cuando lo exija la ley estatal aplicable): podrás solicitar revisión de la respuesta negativa; indicaremos canal y plazo.

13. Menores

13.1 No dirigimos el Sitio a menores de 13 años ni recabamos deliberadamente sus datos sin cumplir requisitos legales (p. ej., consentimiento verificable del representante).

13.2 Para contratar: ≥ 18 años o consentimiento verificable del representante legal (quien asume obligaciones de la operación).

14. Incidentes de seguridad y notificaciones

14.1 Activamos el Plan de Respuesta a Incidentes (PRI): detección → contención → análisis → remediación → notificación (cuando proceda) → post-mortem.

14.2 Cuando la ley lo exija, notificaremos a autoridades y/o afectados con: descripción de hechos, alcance, riesgos, medidas adoptadas y recomendaciones (incluida la rotación de credenciales).

14.3 Conservación de evidencia: logs, snapshots y hashes por el tiempo estrictamente necesario para investigar y acreditar actuaciones.

15. UGC, propiedad intelectual y DMCA

15.1 El Contenido Generado por el Usuario (UGC) puede usarse conforme a la licencia prevista en los T&C (alojamiento, reproducción, comunicación pública en canales oficiales).

15.2 Atendemos avisos DMCA (notice & takedown); los requisitos del aviso y el agente designado figuran en los T&C.

16. Bases contractuales y prueba de aceptación

16.1 La aceptación de esta Política y de los T&C se formaliza válidamente por medios electrónicos (E-SIGN Act, UETA cuando aplique, Ley de Firmas Electrónicas de PR).

16.2 Conservamos evidencias: fecha/hora, IP/user-agent, versión del texto y hash de la versión aceptada.

17. Cambios a esta Política

17.1 Podremos modificar/actualizar la Política por razones legales, técnicas u operativas. La versión vigente será la publicada en el Sitio con su fecha.

17.2 Cuando corresponda, enviaremos aviso general a usuarios registrados. El uso continuado implica conocimiento de la versión actual sin menoscabo de derechos imperativos.

ANEXO I — Tabla de Conservación (orientativa)

- **Cuenta/Perfil:** vigencia + hasta 2 años.
- **Facturación/contabilidad:** 5–7 años.
- **Logs autenticación:** 12 meses; **eventos críticos:** 24 meses; **incidentes:** hasta cierre + legal.
- **RMA/Reclamos:** hasta cierre + prescripción aplicable.
- **Marketing:** mientras consentimiento/relación o hasta opt-out.

ANEXO II — Marco de seguridad (síntesis operativa)

- **Controles:** TLS, cifrado en tránsito/en reposo (cuando aplique), MFA, mínimo privilegio, WAF/IDS/IPS, rate-limiting/anti-bot, segregación prod/test, backups, gestión de parches, escaneos de vulnerabilidades, pentest cuando corresponda.
- **Gestión de secretos:** bóvedas, rotación, no embebidos.
- **Logs:** autenticación (éxito/fallo), MFA, cambios sensibles, pagos (ID transacción, no PAN/CVV), webhooks firmados, decisiones de cookies, aceptación T&C (hash).
- **Integridad probatoria:** sellado temporal y hashing de paquetes de evidencia.

ANEXO III — Avisos sectoriales y compatibilidades

- **HIPAA:** no somos “covered entity” ni “business associate”; salvo pacto/actividad específica, HIPAA no aplica.
- **CAN-SPAM/TCPA:** marketing por e-mail/SMS exige base legal válida; SMS requieren consentimiento expreso por escrito; “STOP” para baja.
- **Publicidad:** cumplimos FTC Endorsement Guides/Green Guides en lo aplicable; divulgación de relaciones materiales con endorsers; sustanciación razonable de claims; coherencia con tus T&C (publicidad responsable).
- **Controles de exportación/OFAC:** no operamos con jurisdicciones/personas sancionadas.

ANEXO IV — Aviso de Derechos por Jurisdicción (EE. UU. + UE/RU)

A) Consumidores de California (CPRA) y estados con leyes análogas (VA/CO/CT/UT, etc.)

A.1 Categorías CPRA que podemos tratar (según el caso): identificadores (A), registros de cliente (B), información comercial (D), internet/actividad de red (F), inferencias limitadas (H) sin perfilado invasivo; no tratamos categorías sensibles salvo verificación mínima e informada.

A.2 Finalidades: ver Sección 3. **Retención:** ver Anexo I. **Fuentes:** directas, automáticas, pasarelas/transportistas.

A.3 Divulgaciones a terceros: sólo a encargados para fines operativos; no vendemos datos personales ni realizamos “sharing” para publicidad conductual cross-context sin tu opt-in previo (cuando aplique) y opt-out siempre disponible.

A.4 Derechos: conocer/acceder, corrección, eliminación, opt-out de ventas/sharing (si alguna vez aplicara), no discriminación. Señal de GPC (Global Privacy Control): la respetamos para flujos sujetos a CPRA cuando se vincule de forma verificable. Apelación: canal de revisión disponible en caso de denegación (se informará en la respuesta).

A.5 Menores: no vendemos/compartimos datos de menores de 16 años.

B) Espacio Económico Europeo/Reino Unido (GDPR/UK GDPR)

B.1 Responsable: Empresa (datos en encabezado). DPO/Privacy Lead: designado internamente; contacto vía sales@coelnigerianojj.com.

B.2 Bases: art. 6.1 a), b), c), f) según corresponda (véase Sección 2). Interés legítimo documentado con prueba de balance.

B.3 Transferencias: cuando corresponda, SCC/UK IDTA u otro instrumento válido + evaluación de riesgos del destino.

B.4 Derechos: acceso, rectificación, supresión, limitación, oposición, portabilidad, y a no ser objeto de decisiones exclusivamente automatizadas con efectos jurídicos similares (no realizamos este tipo de decisiones). Reclamación: autoridad de control competente; te invitamos a contactarnos primero.

B.5 Conservación/Seguridad: ver Anexos I–II.

Cláusula de entendimiento destacado (resumen ejecutivo para el usuario)

- No vendemos tus datos ni hacemos “sharing” para publicidad conductual sin tu base legal/opt-in cuando sea exigible; opt-out siempre disponible.
- Operamos con pasarelas PCI DSS; no guardamos PAN/CVV.
- Puedes acceder/corregir/eliminar/limitar/oponerte/portar (cuando aplique) y darte de baja de marketing en cualquier momento.
- Tenemos plan de incidentes, logs y controles para proteger tus datos.
- Cookies no esenciales sólo con tu consentimiento en el CMP.