

Operations & Compliance Manual

Regulatory Framework: LOK Article 5.9 & Curaçao Gaming Authority (CGA)

Trillionario • WinTrillions • Trilhardario • LottoKings • Lotosena

This document serves as the official Operations Manual for the company's gaming brands (Trillionario, WinTrillions, Trilhardario, LottoKings, and Lotosena), structured in strict accordance with Article 5.9 of the National Ordinance on Games of Chance (LOK).

Article 5.9

The holder of a licence granted pursuant to Article 5.1, first paragraph, must at all times maintain an operations manual containing information about the manner and extent of compliance with the provisions laid down by or under this National Ordinance, as well as the rules and restrictions attached to the gaming licence, including in any case:

- a. a description of the games of chance offered as part of its operations, the payment possibilities, stakes, payouts, software, and elements determining the outcome;*
- b. a description of the periodically used test methods for quality monitoring;*
- c. the method of storing personal data and other data of participants;*
- d. a description of visual elements shown to the participant as part of the operation through the gaming website or other software application;*
- e. a description of technical measures taken to prevent the admission of natural persons who, under the National Ordinance, are not permitted to participate in the games of chance offered as part of the operation;*
- f. a schematic representation of the technical infrastructure, as well as a description of restoration possibilities in the event of a technical emergency occurring in relation to the operation;*
- g. a description of how the principles of responsible gaming provision have been implemented in the operation, taking into account the provisions of Articles 2.2, third paragraph, 5.4, and 5.6;*
- h. the most recent text of the general terms and conditions used by the operation;*
- i. a description of how the licence holder settles disputes with participants, taking into account the provisions of Article 5.3;*
- j. the digital records maintained regarding certain critical information about players, their gaming transactions, and their financial transactions, which must be kept available for the CGA at all times on a server of a Tier-IV certified data centre established in Curaçao.*

Each letter bullet corresponds to the subitem within Article 5.9 of the LOK.

Content

a. Description of Games.....	4
Lottery Products.....	4
Casino Products.....	4
Provider Selection Criteria.....	5
Commercial and User-Facing Criteria.....	5
Pricing.....	6
Payment & Transaction Management.....	6
Player Deposit & Account Funding.....	6
Balance Top-Up.....	7
Payment Method Selection.....	7
Direct Payment on Purchase: Product Purchases.....	8
Data Requirements, Security & Identity Verification for Financial Transactions.....	8
Withdrawal (Cash-Out) Procedure & Payout Execution.....	9
b. Test Methods for Quality Monitoring.....	10
UX, Content and Campaign Quality Checks.....	10
c. Method of Storing Personal Data.....	11
SRE, Deployment & Compliance.....	11
d. Description of Visual Elements.....	13
g. Responsible Gaming Provision.....	16
Mandatory Requirements (Regulatory Reference).....	16
Designation of Compliance Officer.....	16
Prevention of Underage Gambling & Age Verification (Section 5).....	16
Player Information and Accessibility (Sections 6.1–6.4).....	17
Self-Assessment & Gambling History (Section 7).....	17
Behaviour Tracking (Section 8).....	18
Cooling Off and Self-Exclusion.....	18
Cooling Off Protocol (Section 9.1).....	18
Self-Exclusion Protocol (Section 9.2).....	19
Operator-Initiated Exclusion (Section 9.3).....	19
Limits (Section 10).....	19
Training and Staff Readiness (Section 11).....	20
Consumer Advertising and Marketing (Section 12).....	20
i. Description of Settlement of Disputes.....	21
Policy Overview & Regulatory Framework.....	21
Step-by-Step Resolution Process.....	21
Step 1: Frontline Contact (Email & Chat).....	21
Step 2: Official Escalation Form Submission.....	21

Operational Timelines	22
Stream A: Responsible Gaming (RG) Complaints	22
Stream B: All Other Complaint Types	22
Categorization, AI Guardrails, and Final Determinations	22
Artificial Intelligence (AI) Guardrails	22
The Final Written Determination	23
Alternative Dispute Resolution (ADR) Protocol	23
Record-Keeping & Reporting	24
Bi-Annual Reporting	24
Data Retention	24
e. Admission and Participation Restrictions	24
Fraud Management System (FMS) & Security	24
Notifications, Calls & Alerts	25
f. Representation of the Technical Infrastructure	27
System Architecture & Component Topology	27
Financial Processes & Order Management	27
Gaming Operations & Draw Management	28
Architectural Foundation & Data Flow	28
Game Integrations & Web Updates	28
Fulfillment, Costs, and Player Benefits	28
Game Integration Architecture	29
Payment Orchestration & The “Cascade” Engine	29
Payouts & Auto-Claims	30
Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)	31
1. Workforce Continuity & Mobility	31
2. Core Infrastructure & Database Resilience	31
3. Domain Topology & Attack Mitigation	31
4. Payment Engine & Financial Continuity (Cascade)	32
5. Game Provider Contingency	32
6. Regulatory Compliance Resilience (KYC/AML & Fraud)	32
7. Crisis Management Protocols, Monitoring & Alerts	32
8. Immediate Deployment Recovery (Zero Downtime & Rollbacks)	33
Diagram of the technical infrastructure: Attached.	33
j. Critical Digital Records Storage	34
Current State:	34
Interim Technical Infrastructure	34
Justification and System Security of AWS CloudWatch	34

a. Description of Games

The following Marketing input applies to the customer-facing presentation of the gaming products offered through the following brands: Trillionario, WinTrillions, Trilhardario, LottoKings and Lotosena.

From a Marketing and user-facing perspective, the operation offers two main gaming verticals:

- Lottery
- Casino

Within these verticals, the products may have variations depending on the brand, market and product availability.

Lottery Products

Users may access lottery-related products through the website. These products are backed by the results of official lotteries and may be presented as individual lottery tickets, ticket packages, Lottery Teams participations or Lotería Nacional products, depending on the brand and market.

The customer-facing lottery interface displays the following core details:

- Lottery name
- Jackpot or estimated prize amount, when applicable
- Draw date
- Product type, such as individual ticket, package, Lottery Team participation or Lotería Nacional product
- Number of lines, entries, tickets or participations, when applicable
- Promotional discount or offer, when applicable
- Prices and the final amount are shown to the user before purchase confirmation.*
- Purchase call to action
- Relevant terms, conditions or explanatory messages

* Depending on the selected payment method, country, processor, or transaction flow, additional charges may apply.

IT Reference: For the technical lottery integration, draw processing, provider result collection and payout trigger logic, please refer to the IT Manual, Section 3 — Gaming Operations & Draw Management and Section 4 — Game Integration Architecture / Lottery Integration (Messenger Model).

Casino Products

Users may access online casino games through the Casino section of the website.

The company does not develop its own casino games. Casino games are provided by certified third-party game providers, aggregators or platforms. These may include providers such as Evolution, Pragmatic Play, SoftSwiss, among others, depending on availability, brand, market and integration.

From a customer-facing perspective, casino games may be displayed through:

- Casino lobby.
- Game categories.
- Game thumbnails.
- Game name.
- Provider name or logo, when applicable.
- Featured games.
- New games.
- Popular games.
- Promotional placements.
- Play button or access button.

The outcome of casino games is not determined by Marketing and it is not generated by internally developed Marketing assets. Game logic, RNG, game mechanics, payout behaviour, certifications and technical operation remain under the responsibility of the certified provider, aggregator, IT, Operations or the relevant technical owner.

***IT Reference:** For the technical casino integration, please refer to the IT Manual, Section 4 — Game Integration Architecture / Casino Integration.*

Provider Selection Criteria

Commercial and User-Facing Criteria

From a Marketing perspective, provider selection is assessed based on customer experience, product relevance, brand fit and commercial value.

Marketing may consider the following criteria:

- Provider certification, licensing or compliance status, as validated by the relevant internal area.
- Provider reputation and market recognition.
- Quality and attractiveness of the game catalogue.
- Relevance of the games for the target markets.

- Availability of well-known or high-performing titles.
- Variety of game categories.
- Availability of promotional materials, images, game information and campaign assets.
- Compatibility with CRM actions, promotions, featured placements and campaign mechanics.
- User experience, including mobile usability, loading experience and clarity of game presentation.
- Technical compatibility, as validated by IT or the relevant technical team.
- Commercial performance once live, including user engagement, conversion, retention and revenue contribution.
- Market availability and restrictions by country or brand.

Marketing does not validate RNG, backend certification, or provider infrastructure, but the company hires B2B licenced providers to comply with industry standards and regulations.

***IT Reference:** For the technical provider integration model, please refer to the IT Manual, Section 4 — Game Integration Architecture, particularly the casino integration through certified aggregators and the lottery provider model.*

Pricing

Pricing is defined by the Marketing team and approved by the COO. Prices displayed on the website are final customer-facing prices and may vary depending on the lottery, product type, currency, market, and active promotions. Any additional fees or charges must be clearly shown before checkout.

Payment & Transaction Management

This procedure establishes the protocols for secure transactional funding and the mandatory logging of player deposits and inbound wealth.

Player Deposit & Account Funding

There are two payment triggers:

- Balance Top-Up, where the client adds funds using their preferred payment method into their balance account for future purchases.
- Direct Payment on Purchase, where clients select products to buy and pay for them directly through the payment method of their choice.

To comply strictly with AML/CFT criteria, it is mandatory that players are logged in and authenticated before executing any payment deposit or withdrawal.

Balance Top-Up

- **Direct Wager Prohibition:** Players are strictly prohibited from placing Casino bets directly via external payment methods; an initial account balance funding is mandatory.
- **Interface Access:** The player accesses the “Balance Management” section within their user account to initiate the process of topping up their account.
- **Selection Iframe:** Client confirms deposit. The system deploys an iframe displaying predefined deposit increments or allowing for manual entry.
- **Cashier Access:** Upon confirmation of the deposit amount, the system redirects the user to a secure digital cashier.

Payment Method Selection

Flow 1: Credit and Debit Card Processing

- The system supports bank-issued cards (e.g. Visa, Mastercard) to facilitate immediate electronic transfers.
- Players input card credentials or select previously stored payment data.
- The issuing bank may trigger a 3D Secure (3DS) challenge to validate the transaction.
- A real-time on-screen notification informs the client whether the transaction is approved or declined.

Flow 2: Alternative Payment Methods (APM)

- This flow includes non-card options such as e-wallets, vouchers, or digital provider balances.
- The system redirects the player to the third-party provider’s secure environment to complete the transaction.
- Following processing, the player returns to the cashier where a real-time on-screen notification informs the client whether the transaction is approved, declined, or on hold pending completion of instructions for cash-based payments at authorised partner locations.

Flow 3: Cryptocurrency via QR Code

- The system facilitates digital currency transactions (e.g. Bitcoin, Ethereum) through regulated Virtual Asset Service Providers (VASPs).
- A unique transaction QR code and a corresponding destination wallet address are generated per request.
- The player scans the code with a personal wallet to authorise the transfer.
- The system monitors the blockchain for the required network confirmations prior to updating the account balance.

- A real-time on-screen notification informs the client whether the transaction is approved, declined, or pending. Crypto payments may take longer to be cleared by the corresponding financial institution.

The in-house built cashier is connected to the payment processing supplier through a server-to-server integration. The PSP provides credentials associated with the merchant account. The information sent complies with PSD2 protocols.

IT Reference: For further information refer to the IT Manual, Section 5 — Payment Orchestration & The “Cascade” Engine.

Direct Payment on Purchase: Product Purchases

- Selection & Bet Amount: The player selects specific raffle tickets or lottery numbers according to their preference.
- Bet Confirmation: Following selection, the client confirms the wager explicitly to proceed to the settlement stage.
- Order Summary: The client is directed to the cashier, where the total expenditure and complete details of the selected product are displayed.
- Payment Flow: At this stage, the payment flows detailed in the Payment Method Selection section repeat to finalise the purchase.
- Outcome Notification: A real-time on-screen notification informs the client whether the transaction is approved or declined.

For all purchases — either direct payment or using balance funds — a unique digital record is generated for every gaming transaction, linking the payment directly to the game’s outcome-determining elements as per provider criteria and the player.

IT Reference: For further information refer to the IT Manual, Section 5 — Payment Orchestration & The “Cascade” Engine.

Data Requirements, Security & Identity Verification for Financial Transactions

The system requires clients to input data according to the AML Policy and security and risk management requirements set by payment processing providers as well as financial institutions involved in the payment process.

The collected data is used to run AML and prevention of funding of terrorism checks, as well as for the prevention of fraudulent transactions. The main pillars of these requirements are:

- Customer Data Collection: Users provide the full cardholder name, expiry date, and CVV code. For bank transfers and virtual wallets, the system captures the originating account/IBAN or the registered email.

- **Withdrawals (Pay-outs):** Prior to authorisation, a “Closed-Loop” policy is enforced, requiring funds to return to the original source. Mandatory documentation includes updated Proof of Identity and Proof of Address. Source of Funds (SOF) declarations are required for high-value transactions.
- **Back-End Monitoring:** The system records Device Fingerprinting (IP, geolocation, unique IDs), Transaction Velocity, and comprehensive Audit Trails (including processor response codes and timestamps).
- **External Verification:** Fraud prevention checks (e.g., Ethoca) are performed by specific Payment Service Providers (PSPs), including checks of international databases to review the client’s payment history with other merchants.
- **3D Secure (3DS) Flow:** Issuing banks and some PSPs follow PSD2 protocols to prevent fraudulent or risky transactions, performing card-associated ID challenges through SMS or biometric approval.
- **Live Identity Verification (Liveness Check):** Triggered by third-party partners for clients meeting defined criteria — including but not limited to first depositors or those who reach risk thresholds. The process includes Document Capture (OCR), Liveness Detection (Video or Selfie), and biometric matching.
- **Internal AML/Risk:** Third-party tools perform Anti-Money Laundering (AML) checks in compliance with risk policies.

Withdrawal (Cash-Out) Procedure & Payout Execution

- **Withdrawal Request Initiation:** The player must access their user account and navigate to the “My Wallet” section. The user selects “My Winnings” followed by “Balance for Withdrawal”.
- **Withdrawable Funds:** The system displays funds available for withdrawal and the list of withdrawal methods available. These funds strictly exclude any bonus funds or special loyalty points.
- **Formal Request:** The client must submit a formal request via the interface, entering the amount they wish to withdraw and selecting a method from the list before pressing the submission button.
- **Capture of the Request:** Upon executing this action, a formal request will be created in the customer’s transactional history and will be subject to internal review processes prior to execution.
- **Closed-Loop Preference:** Funds are required to return to the original payment source used for the initial deposit, up to the total amount of the original deposit(s), prior to any alternative method being authorised.
- **Balance Update:** The withdrawal request amount is automatically deducted from the client’s available balance.
- **Compliance & AML Review:** Automated controls are performed by the relevant operational systems and tools. Compliance performs review and evaluation activities, where applicable, in line with the Company’s Anti-Money Laundering Policy (AML/P). Withdrawal approval and

execution are performed according to the applicable operational procedures and system workflows.

- Final Settlement: If approved, funds are transferred and settled according to the established Terms & Conditions (T&Cs) and in observation of the payment provider's settlement times. An email is automatically sent to the customer showing the transaction details.
- Digital Logging: Every payout transaction is uniquely logged in the client's transaction history as a digital record, including relevant timestamps.

These digital records, together with the underlying transaction data, serve as primary evidence for dispute resolution and are maintained in a format ready for inspection by the Curaçao Gaming Authority (CGA) according to the LOK.

***IT Reference:** For further details on the AML/CFT procedures please refer to the AMLCFT Operational Procedures Manual vJune2026.*

b. Test Methods for Quality Monitoring

UX, Content and Campaign Quality Checks

Marketing performs recurring user-facing checks focused on content accuracy, campaign visibility, promotional consistency and user experience.

These checks are operational Marketing reviews and should not be understood as formal technical QA documentation. Marketing checks may include:

- Website and promotional visibility checks: Marketing reviews that banners, sliders, promotional cards, campaign placements, lottery highlights, casino featured games and landing pages are correctly displayed from the user-facing side.
- Price and promotion communication checks: Marketing reviews that user-facing promotional information is clear and consistent, including:
 - displayed prices,
 - promotional discounts,
 - bonus or offer descriptions,
 - campaign labels,
 - terms and conditions,
 - calls to action,
 - destination links, and
 - explanatory messages.

Where a product or promotion displays a price, Marketing checks that the price communication is clear and aligned with the intended campaign. If additional fees may apply depending on the payment method, processor or transaction flow, this should be reflected where applicable in the relevant user-facing information.

- **Content and copy checks:** Marketing reviews campaign texts, promotional messages, lottery descriptions, casino promotional content, subject lines, preheaders, disclaimers, calls to action and translations to ensure communication is aligned with the Responsible Gaming protocols, clear, accurate and consistent with the approved campaign. Responsible Gaming Protocols include but are not limited to a clear sign indicating the prohibition for underage people and access and acceptance of the last approved version of the Terms and Conditions.
- **Link and CTA checks:** Marketing verifies that campaign buttons, banners, promotional links, lottery links, casino links, landing page links and CRM links redirect users to the intended destination.
- **Mobile and desktop UX checks:** Marketing reviews how key promotional and gaming elements are displayed on desktop and mobile, including readability, image quality, layout, CTA visibility and general user journey clarity.
- **Campaign QA before launch:** Before campaigns are sent or published, Marketing checks the final creative pieces, language version, promotional conditions, links, images and final customer-facing message.
- **Post-publication checks:** After publication or campaign launch, Marketing may verify that the campaign, slider, promotion, email, push notification or website element is live, visible and working correctly from the user-facing side.

***IT Reference:** Technical QA, payment testing, system performance, integrations, security controls, provider API testing and backend data processing as well as cart integrity controls please refer to the IT Manual, Section 2 — Financial Processes & Order Management / Cart Checker.*

c. Method of Storing Personal Data

SRE, Deployment & Compliance

Maintenance requires strictly manual processes to ensure zero operational downtime.

- **Deployment Workflow:** Code is compiled via mvn clean install on JDK 1.8 to generate trillonario-jar-with-dependencies.jar. Production releases require a mandatory backup before hot-swapping the binary and restarting Port 2012.
- **GDPR & Data Privacy:** Implements “Privacy by Design.” PII is encrypted at rest (AES-256), and financial data is obfuscated to maintain PCI-DSS compliance. Right to Erasure is supported via automated scripts.

- External Gateways: Manual gateways require strict encryption (AES/CBC/PKCS7Padding for card details) and SHA-256 HMAC digital signatures in the x-requested-with headers.
- Live Monitoring: Operations teams monitor metrics via Prometheus/Grafana (Micrometer) and distributed logs via the ELK Stack (Kibana). Resilience4j Circuit Breakers prevent cascading failures during provider downtimes. Sales and blockings are tracked via internal portals.
- Logs: AWS CloudWatch — A 24/7 coverage policy ensures that at any given time at least one person is available to supervise the operation of the site, solve any disruption in the service, or escalate in the case of a major disruptive event.

d. Description of Visual Elements

Participants may be shown different visual elements throughout the gaming websites and CRM communications. These elements are designed to guide the user journey, present available products, communicate prices and promotions, and support navigation across the platform.

The main visual elements may include:

- Homepage elements
 - Main banners.
 - Promotional sliders.
 - Featured lottery products.
 - Featured casino games.
 - Jackpot highlights.
 - Promotional blocks.
 - Calls to action.
- Lottery presentation elements
 - Lottery cards.
 - Jackpot cards.
 - Draw dates.
 - Prize amounts.
 - Ticket, package or Lottery Team participation selectors.
 - Number of lines, entries, tickets or participations, when applicable.
 - Prices displayed to the user before purchase confirmation.
 - Promotional labels.
 - Purchase buttons.
 - Explanatory messages related to the lottery product.
- Casino presentation elements
 - Casino game thumbnails.
 - Game cards.
 - Game names.
 - Provider names or logos, when applicable.
 - Casino category icons.
 - Filters.
 - Search bars.
 - Play buttons.
 - Featured game sections.

- Promotional casino placements.

Casino games are shown as third-party certified provider games integrated into the platform. Marketing manages the user-facing presentation but does not manage the underlying game logic, RNG, technical outcome or provider system.

- Promotional elements
 - Promotion cards.
 - Bonus banners.
 - Discount messages.
 - Campaign labels.
 - Offer tags.
 - Countdown messages, when applicable.
 - Popups.
 - Web push prompts.
 - Landing page visuals.

Where promotions include prices, discounts or bonus conditions, Marketing reviews the clarity of the user-facing communication.

- Navigation elements
 - Menus.
 - Category tabs.
 - Filters.
 - Search bars.
 - Buttons.
 - Icons.
 - Breadcrumbs.
 - Links to key sections of the website.
- Informational and compliance-related elements
 - Terms and conditions links.
 - Responsible gaming messages.
 - Age restriction notices.
 - Payment method icons.
 - Security or trust messages.
 - Help and support links.
 - Explanatory tooltips, when applicable.
- CRM and communication elements. Marketing may also coordinate or review user-facing CRM communication elements, such as:

- Email creatives.
- Push notification content.
- In-site campaign messages.
- Promotional visuals sent through CRM platforms.
- Campaign landing pages.
- Promotional terms communicated through CRM channels.

Marketing is responsible for the creation, review or coordination of many of these visual and communication elements, ensuring that they are clear, aligned with the brand, consistent with the promotion and understandable for users.

IT Reference: For the technical casino display and integration model, please refer to the IT Manual, Section 4 — Game Integration Architecture / Casino Integration.

g. Responsible Gaming Provision

This manual details how the company complies with the operational requirements set out in the Responsible Gaming Policy for Licenced Operators by the CGA (“Policy”) outlined by the Curaçao Gaming Authority (CGA).

Numbers detailed below correspond to the section numbers in the Responsible Gaming Policy.

Mandatory Requirements (Regulatory Reference)

- Age verification (Section 5)
- Information accessibility (Section 6)
- Player self-assessments (Section 7)
- Behaviour tracking (Section 8)
- Cooling-off Periods (Section 9.1)
- Self-exclusion (Section 9.2)
- Deposit limits (Section 10)
- Consumer Advertising and Marketing (Section 12)
- Training of employees (Section 11)

Designation of Compliance Officer

A senior member of the team, separate from the AML/CFT Officer, has been designated as Compliance Officer responsible for implementing and enforcing the Responsible Gaming policy. The Officer provides Responsible Gaming (“RG”) reports as required by the regulation.

Prevention of Underage Gambling & Age Verification (Section 5)

The company strictly prohibits any minor (individuals under the age of 18) from being given the opportunity to participate in games of chance on the platforms.

- **Registration Validation:** Upon a visitor’s first interaction with the websites, an explicit age-gate modal triggers, asking: “Are you 18 years old or older?”. If the person clicks “NO”, the system redirects them to a restricted page, completely stopping platform navigation.
- **Rigorous Age Verification:** During account registration, players must self-attest their age by entering their date of birth and ticking a designated checkbox. The client’s registered data is then processed through Sumsud services to cross-reference against official government lists and electoral registers.
- **Thresholds and Document Checks:** A valid government-issued ID check (such as a passport, national ID, or driver’s licence) is deployed. This check is strictly triggered upon

reaching specified financial thresholds and, without exception, prior to completing the first withdrawal.

- Underage Account Handling: If the company becomes aware that a player is a minor, compliance protocols dictate that the account must be closed immediately. All deposits made by the player are returned regardless of win or loss, any accumulated winnings are forfeited, and clear records of the verification outcome are preserved for regulatory review by the CGA.

Player Information and Accessibility (Sections 6.1–6.4)

The company ensures that comprehensive information regarding responsible gambling and gambling addiction is prominently displayed and easily accessible in English, as well as the target market languages (Spanish and Portuguese).

- 6.1 & 6.2 Homepage and RG Section Accessibility: A clear, identifiable, and visible link labelled “Responsible Gaming” is permanently displayed within the footer of all operating domains. This link leads directly to the dedicated Responsible Gaming Statement page.
- 6.3 Terms & Conditions Inclusion: The Responsible Gaming Section and corresponding tools are explicitly referenced and integrated within the website’s Terms & Conditions, which remain no more than one click away from the homepage.
- 6.4 Footer Information Requirements: The footer contains all essential transparency details required by the CGA: a clear “+18” visual prohibition logo, the corporate name and registered address, the official licence application number, a text statement confirming regulatory oversight, and the active CGA Digital Seal (GCB dynamic seal).

Self-Assessment & Gambling History (Section 7)

The company provides structured tools and transparency metrics to empower players to monitor and regularly evaluate whether their gambling remains within healthy limits.

- Transaction History Records: Registered participants can access a detailed record of their betting and wagering history, including granular transaction timestamps, deposits, and withdrawals, directly within their Customer Account interface, covering at least the last six months. Requests for older historical transaction periods can be made via customer support, with a target delivery of within 10 working days.
- Scientifically Recognised Screening Tools: The dedicated Responsible Gaming page hosts the CAGE Questionnaire (Adapted for Gambling). Clear, neutral guidelines are published to help players interpret their answers.
- Support Recommendations and Referrals: The sites explicitly recommend that any player may self-assess using the responsible gambling questionnaire and other dedicated third-party sites, including a direct hyperlink to the Gamblers Anonymous 20-question quiz.

Behaviour Tracking (Section 8)

The company maintains functional, active monitoring frameworks to identify at-risk individuals and implement structured intervention strategies to mitigate gambling-related harm.

- 8.1 Key Monitoring Factors: Frontline staff (including Customer Support representatives and VIP Managers) track accounts for simultaneous indicators of distress, including shifts in deposit and wagering frequency, repeated failed transactions due to insufficient funds, multiple instances of reversing withdrawals, extended play sessions, and frequent modifications to Responsible Gaming tools.
- 8.2.1 & 8.2.2 Profiling and Escalation Protocol: All player-initiated or company-initiated interactions are formally logged in the player's profile. Based on the assigned risk assessment, the escalation protocol includes:
 - Proactively informing the customer of available responsible gaming preferences.
 - If at-risk behaviour persists, enforcing mandatory deposit limits on the account.
 - Temporarily suspending the player's account pending a comprehensive compliance evaluation.
 - For cases of severe or persistent risk, applying a permanent company-initiated exclusion. Under no circumstances are these protective interventions misused as a pretext to delay or prevent legitimate player withdrawals.

Cooling Off and Self-Exclusion

Cooling Off Protocol (Section 9.1)

The "Limitations" page, accessible from the homepage, provides direct access to tools that empower players to restrict their own gameplay. The interface displays these options using non-pre-checked tick-boxes, ensuring that players are never guided or influenced toward one option over another.

- Duration Options: Customisable short-term breaks of 24 Hours, 7 Days, 1 Month, or 3 Months.
- Vertical and Brand Options: Players can choose to restrict all wagering activity across the entire brand or isolate the restriction to specific product verticals (Casino or Lottery).
- Actions and Implementation Rules: Restrictions apply instantly upon selection via an online confirmation pop-up. During the break, the account remains active but disabled from selected gambling features, and the customer's funds remain fully accessible for withdrawal.
- Marketing Restrictions: If a player selects the mandatory Marketing Opt-Out, all direct marketing materials are strictly halted, and no bonuses, free play, or incentives may be offered during the cooling-off period.

- **Post-Cooling Off Reactivation:** Accounts regain full capabilities automatically once the selected cooling-off period expires, requiring no manual actions or communication from the player.

Self-Exclusion Protocol (Section 9.2)

From the front end of all websites, players can click the “Self-Exclusion” option within the homepage footer to launch the process. Once redirected to the dedicated page, they log in to verify their identity and complete the brief setup sequence to activate the restrictions immediately.

- **Irrevocable Long-Term Durations:** In compliance with the LOK and CGA guidelines, the company offers long-term, irrevocable self-exclusion terms of 1 year, 3 years, 5 years, 10 years, or a Lifetime.
- **Automated Online Process:** Players are able to initiate and complete the self-exclusion sequence fully online without requiring email communication or prior operator approval. Activation takes effect immediately across all domains, brands, and verticals operating under the licence.
- **Account Enforcement Actions:** The account is closed and the customer can no longer log in. Any pending ante-post wagers are voided and refunded (subject to AML regulations), and remaining cash balances are automatically transferred to the player’s registered payment method.
- **Circumvention and Duplicate Controls:** Robust checking measures within the system detect duplicate accounts and prevent self-excluded individuals from creating new credentials. Known payment methods linked to the individual are blacklisted from future use, and all direct marketing and advertising materials are completely blocked.
- **Reactivation Protocol:** Activation of a self-exclusion is strictly irreversible for its selected duration. Once the timeframe ends, the player must submit an unprompted written request through official customer support channels to unblock their account.

Operator-Initiated Exclusion (Section 9.3)

The company reserves the right to exclude a customer from gaming activities if they display problematic gambling behaviour or engage in fraudulent or criminal acts via the platform. Players are never excluded based on the amount of their winnings. All operator-initiated exclusions are formally documented, and records are retained for at least five years for potential CGA review.

Limits (Section 10)

- **Safer Gambling Boundaries:** We provide a fully functional "Deposit Limits" system within our site settings. Players can define the total amount of money they are permitted to deposit over rolling daily, weekly, or monthly periods.
- **System Constraints and Asymmetrical Logic:** Once a player reaches their defined cap, our system hard-blocks any further deposit attempts until the specified timeframe resets. To

protect players from impulsive changes, our system enforces strict timing logic: requests to increase severity (lower a deposit limit) take effect instantly, while requests to decrease severity (raise or remove a limit) are subject to a mandatory 24-hour waiting period before implementation. Any wagers made prior to setting the limit remain completely unaffected.

Training and Staff Readiness (Section 11)

All frontline personnel who interact directly with customers (Customer Support and VIP teams at a minimum, alongside Marketing personnel) must complete an induction training course on responsible gambling, followed by mandatory annual refreshers.

Delivered by the designated Responsible Gaming contact person and Customer Experience Manager, workshops ensure staff are fully prepared to:

- Recognise signs of gambling distress (such as agitation, aggression, or financial desperation).
- Conduct structured and sensitive conversations with at-risk players.
- Accurately direct vulnerable individuals to international support resources and internal protective tools.

Consumer Advertising and Marketing (Section 12)

All marketing, promotion, and design teams operate under a strict, integrated Marketing Decalogue checklist. The company ensures that advertising materials:

- Do not target vulnerable groups or minors.
- Never portray gambling as a financial investment or a way to achieve financial success.
- Do not misrepresent skill over chance in purely chance-based games.
- Omit any explicit or inappropriate content.

Every piece of marketing communication, including affiliate materials, must feature a clearly visible Responsible Gaming message or slogan.

The company actively communicates its Responsible Gaming Policy to all contracted third parties, requiring strict adherence to these regulatory safety conditions.

i. Description of Settlement of Disputes

Policy Overview & Regulatory Framework

- **Compliance Mandate:** This policy framework ensures a transparent, fair, and efficient process in strict alignment with integrity requirements under Article 5.3 of the National Ordinance on Games of Chance (LOK).
- **Transition Scope:** The policy applies to all players on the company's sites.
- **Player Accessibility:** Players have access to this dispute resolution process completely free of charge. The policy is clearly referenced in the Terms and Conditions and has a dedicated page at just one click from the front end of all sites.
- **The Complaint Window:** Players may lodge a complaint at any time up to six (6) months from the settlement of the bet or the incident about which they are making a complaint.
 - **P2P & Fixed Odds:** For peer-to-peer (e.g., poker) or ante-post fixed-odds betting, the 6-month clock begins after the bet settlement or conclusion of the specific event rather than the placement of the wager.
 - **In-Running Sports Betting:** Customers must be advised that prompt action may be necessary, as specific data may no longer be available after a short period due to the nature of live betting.

Step-by-Step Resolution Process

Step 1: Frontline Contact (Email & Chat)

- **Initiation:** The customer submits an initial complaint within the 6-month window by contacting customer support through Email or Live Chat.
- **Eligibility:** Complaints can only be made by the registered player. Under Article 1.3 section c of the LOK, players are strictly prohibited from selling, donating, renting out, leasing, pawning, or pledging any claims against a gaming licence holder.
- **Immediate Resolution:** If frontline support resolves the issue directly during this interaction, the complaint is recorded as resolved and the task is closed.

Step 2: Official Escalation Form Submission

If the complaint is NOT resolved during frontline email or chat interactions, the customer must be invited to submit a formal claim using the official Complaint Submission Form.

Mandatory Fields: To be processed, the client must provide:

- Full name, address, and place of residence.
- Account number (if applicable).
- Date of the complaint and date of the disputed event.

- Description of the conduct being disputed (using pre-determined category topics if applicable).

Language Requirements: The form is available in English and in the language of the website/domain that the player is using.

Supporting Documentation: The operator may request additional documentation that the player requires to include as part of the complaint, provided it is reasonable in the context of complaint resolution.

Operational Timelines

Once a formal complaint form is submitted, the following timeline is applied:

Stream A: Responsible Gaming (RG) Complaints

- Within 2 Days of Receipt: Confirm receipt in writing, provide an explanation of how the complaint will be processed, and provide notice of the average timeline for resolution.
- Target Resolution: Best efforts to resolve these cases within five (5) business days.
- Permitted Extensions: If more time is needed, the player is informed of the delay, which cannot exceed two weeks. If the delay is due to a slow response from the player, the period may be extended by no more than a further two weeks.
- Commentary: Any complaint regarding vulnerable players, the availability or timely implementation of self-exclusion or cooling-off periods, and their mandated consequences are prioritised due to potential impacts on player well-being.

Stream B: All Other Complaint Types

This applies to standard disputes regarding deposits, withdrawals, bonus terms, account restrictions, KYC, technical issues, or game outcomes.

- Within 1 Week of Receipt: Confirm receipt in writing, provide an explanation of how it will be processed, and provide notice of the average timeline for resolution.
- Standard Resolution: The complaint will be assessed and a response provided to the complainant within four (4) weeks.
- Permitted Extensions: If necessary, due to complexity or lack of information, this period may be extended once by an additional four (4) weeks, with prior written notice to the player.

Categorization, AI Guardrails, and Final Determinations

Artificial Intelligence (AI) Guardrails

The company may use AI to assist in solving complaints, subject to the following strict conditions:

- **Human Only Rule:** Once a complaint has been identified as pertaining to Responsible Gaming, communications with the player must be conducted by a human, not AI.
- **Complex Cases:** Complaints that can be reasonably considered as complex must be dealt with by a human, not AI.
- **Monitoring:** AI utilisation must be monitored to ensure solutions and recommendations are reasonable and consistent across players with like-for-like complaints.

The Final Written Determination

A player will always receive a final determination of their complaint in writing. The response will be one of the following:

- **Reasoned Final Assessment:** A detailed final outcome/resolution of the complaint with supporting evidence if applicable.
- **Rejection for Lack of Information:** Detailed reasons for not handling the complaint. If additional information was requested within the initial four-week window and the complainant failed to provide it, the complaint may be rejected.
- **Escalation Right Notice:** If the player is unsatisfied with the resolution, the client will be informed that they may escalate the matter to an independent Alternative Dispute Resolution (ADR) entity.

Alternative Dispute Resolution (ADR) Protocol

- **Mandatory Provision:** An independent ADR services provider will be offered to the player in accordance with the ADR Policy. Full details of the process will be included in the Terms and Conditions once the ADR is defined.
- **Operator Costs:** If a complaint cannot be resolved internally, players are entitled to escalate the matter free of charge. The operator will bear all costs of the ADR process.
- **Abuse Parameters:** If the operator sets ADR parameters to prevent abuse, each case must still be assessed on its own merits and taken seriously regardless of the monetary value involved.

Finality Rules:

- Once the ADR process is completed, it cannot be recommenced by either the player or the operator with a different ADR entity.
- If the player drops out of the ADR process after it has already begun, they do not have the right to resurface the dispute in the future.
- The operator must not restrict the rights of the player to take subsequent legal action unless mutually agreed under specific terms of the ADR.

Record-Keeping & Reporting

Bi-Annual Reporting

The operator submits reports to the CGA on January 15th and June 15th based on complaints submitted through the official Complaint Submission Form. The reports summarise:

- Total number of complaints made.
- Total number of settled complaints (upheld and rejected).
- Number of pending or unresolved complaints.
- Number of complaints by category.
- Number referred to ADR.
- Number and detail of complaints for which a player has taken legal action.

Data Retention

Records of unresolved complaints and/or complaints that have been escalated to ADR or legal proceedings must be kept for the lesser of five (5) years or the relevant time stipulated by data protection, statute of limitations, or other relevant laws.

The CGA reserves the right to request access to records of complaints received as well as disputes pending resolution at any time.

Commentary: According to the regulation the CGA will not resolve or make decisions on individual player complaints regarding gambling transactions. However, the company will not restrict the player's ability to contact the CGA directly regarding matters such as malpractice, breach of licence conditions, or whistleblowing.

e. Admission and Participation Restrictions

Fraud Management System (FMS) & Security

- The FMS is a multi-layer gatekeeper directly integrated into the Cashier component, further strengthened by a robust Identity Verification (KYC/AML) ecosystem managed via Sumsub.
- Risk & Enrichment: Utilises Maxmind minFraud for BIN enrichment and risk scoring. A score of 50+ triggers a manual "Fraud Alert".
- Rule Implementation: `class.fmsinit.php` executes queries across User, Order, Payout, and FMS data groups. Rules trigger punitive actions via `class.fmswrapper.php`. Adding new rules mandates a Cashier recompilation.
- Duplicate Detection: Scans registrations and coupon usage permanently. Linking to accounts with chargebacks or fraud inherits "High Risk" (Red) status. Related accounts may be restricted as "Potential Risk" (Orange).

- These classifications represent operational fraud and risk indicators used by the Fraud Management System (FMS) and do not constitute the AML/CFT customer risk classification applied under the Company's AML/CFT Risk Assessment Framework.
 - KYC Verification Levels: Identity validation operates on two primary levels depending on the data:
 - First Level (first-level-check-birth): A silent REST API check runs when a user completes their profile (First name, Last name, TIN, Country of birth). If approved ("GREEN"), the user continues normally.
 - Second Level (id-poa-verification): If a user is manually marked as "Under Review" or exhausts 3 automatic API verification attempts, the frontend deploys the secure Sumsu WebSDK IFrame. This is used for capturing hard documentation (ID, Passport) and Proof of Address, and remains active for 30 days.
- AML & Sanctions Screening: The system logs detailed rejection reasons. For Anti-Money Laundering (AML) compliance, the system actively captures and categorises severe risks using tags such as:
 - kyc_pep: Politically Exposed Persons, adverse media.
 - kyc_sanctions: Global sanction lists, criminal records.

These indicators prompt additional risk-based review and evaluation activities where applicable, without automatically implying a restrictive measure or a negative outcome.

- Integration Security: To open the frontend WebSDK IFrame, the backend must generate an Access Token by creating a digital signature using the hash_hmac('sha256') algorithm and a shared secret. Conversely, when Sumsu sends status updates (Webhooks), it signs the payload with HMAC-SHA256. The system recalculates this signature and compares it against the X-Hub-Signature HTTP header to certify the message is authentic before processing.
 - Webhook Processor & Automated Decisions: The dedicated webhook receiver is built on Java 21, Spring Boot, and Spring Data. It immediately persists all events in MongoDB for auditing. The applicantReviewed webhook triggers the automated business logic:
 - Verification Successful: If the result is "GREEN" and "completed", the user's status updates to "verified" in the database, and an internal success email is dispatched.
 - Final Rejection: If the result is "RED" with a "FINAL" rejection type (e.g., sanctions match), the system executes usersService.failed, updates the status to "failed", and sends an internal alert.
 - Rejection with Retry: If the result is "RED" with a "RETRY" type (e.g., blurry photo), the system calls usersService.retry(userId), updates the status to "retry", and triggers an internal notification that the user must try again.

Notifications, Calls & Alerts

- Automated Mails: Dispatches HTML templates for purchase confirmations, wheels, syndicates, and draw results.
- Admin Alerts: Operations receives system emails for DB errors, provider API failures, or carts stuck in special draws.
- Welcome Calls: The Call Centre assigns new leads every 5 minutes based on language (ES, EN, PT, FR, DE). It prioritises Mexican leads and VIP affiliates while excluding specific geographies like Asia and Africa.

f. Representation of the Technical Infrastructure

System Architecture & Component Topology

The platform operates under a hybrid ecosystem utilising a Hexagonal / Clean Architecture and Domain-Driven Design (DDD).

- Frontend & Edge Layer: Built with Angular 13, Node.js (14.20.0), and NPM (6.14.17). Uses Server-Side Rendering (SSR) to optimise SEO and initial load times. Operational modules include the Main Site, Investor Panels, Landing Pages, and the Royal Panel (administrative CMS).
- Backend Orchestration:
 - Wrapper RAPI (Golang): Acts as a high-throughput proxy handling initial requests, JWT validation, rate limiting, and request sanitization.
 - RAPI (PHP 5.6–8): Core business logic layer built on Laravel. Manages user accounts, lotteries, and game catalogs.
 - TPPS Core (Java 21 / 1.8): The central transaction engine. Modern modules use Java 21 with Spring Boot, while legacy maintenance remains on Java 1.8.
- Databases and Cache Strategy:
 - MySQL 5.1: Primary transactional DB for TPPS, Trillonario, and FMS.
 - MySQL 5.7: Reserved specifically for high-availability Proxy/RAPI servers.
 - Memcached & Redis: Distributed, low-latency caching for RAPI tokens and serialized ORCA queries.

Financial Processes & Order Management

The backend handles complex transactional lifecycles through automated batch processing and integrity checks.

- Batch Processing: Transactions (Refunds, Voids, Captures, Authorizations) are processed sequentially. The system identifies pending carts and prevents overlap via the `system_settings` table. It generates an XML payload sent via sockets to the Java system for real-time financial execution.
- Cart Checker: Validates statuses (2, 4, 5, 7) for integrity. Checks for negative prices, ensures discounts match promotional points, detects discrepancies in price tables, and flags abandoned carts.
- Automatic Renewals: Periodic tasks handle lotteries, memberships, and raffles. For raffles, the system reserves tickets with the provider before executing the credit card charge. If the charge fails, the subscription is marked as "On Hold".

- **Account & Card Maintenance:** Daily scans identify users with negative balances and no activity for more than 30 days. A monthly process deactivates credit cards that expired the previous month.

Gaming Operations & Draw Management

The platform acts as a bridge between the core user wallet and multiple gaming verticals, supported by a hybrid Hexagonal / Clean Architecture and Domain-Driven Design (DDD).

Architectural Foundation & Data Flow

- **Supporting Languages:** The frontend is built with Angular 13, Node.js (14.20.0), and NPM (6.14.17), utilising Server-Side Rendering (SSR). The backend is orchestrated across three layers: a Golang Wrapper RAPI proxy, a PHP 5.6–8 (Laravel) core logic layer, and a Java 21 / 1.8 TPPS central transaction engine.
- **Data Transmission & Reception:** To prevent disruptions to main customer-facing sites, data is securely channeled through Edge access domains utilising alternative TLDs. Real-time financial executions generate an XML payload transmitted via sockets directly to the Java system for sequential processing.

Game Integrations & Web Updates

- **Casino Integration & Live Web Updates:** Casino games are integrated via Certified Aggregators (e.g., Oryx, Playtech) and embedded into the website using secure IFrames, ensuring game logic remains entirely on the providers' servers. To keep the website updated with live gaming data without requiring a page refresh, the platform utilizes a Seamless Wallet Protocol. This triggers real-time API requests that instantly synchronize and update the player's central balance as they play.
- **Lottery Integration (Messenger Model):** The platform utilizes third-party providers to purchase official physical or digital tickets for international draws.
- **Draw Processing:** When a draw deadline passes, it is marked as "old," the next draw date is calculated, valid pending tickets roll over, and a new sales cycle opens.
- **Scrapers & Integrity:** Automated agents collect official results (winning numbers, jackpots) from providers like Thelotter, Lottorisq, and Mylottoadserv. The Check Integrity module validates that issued tickets match real provider data and that bets stay within min/max boundaries.

Fulfillment, Costs, and Player Benefits

- **Ticket Fulfillment (Raffles & Syndicates):** The system cancels unconfirmed runs, reserves numbers, confirms them, and updates subscription counters. Syndicates distribute ticket endings equally; if reservations fail repeatedly (more than 3 times), execution stops.

- Mexico (Lotenal) Specifics: Ticket images download asynchronously 8 minutes after purchase. Unpaid transactions are released in the Mexican system hours before the draw, followed by weekly DB reconciliations.
- Loading Costs (Fees Handler): A dedicated microservice automatically evaluates and charges additional costs during transactions, dynamically applying a 10% fee for card handling and a 15% fee for cryptocurrency volatility.
- Casino Benefits: Promotional player benefits, such as Freespins, are automatically distributed directly to accounts via the aggregator API.
- Winnings & Auto-Claims: The system automatically processes unclaimed prizes from the past 40 days. Behaviour 1 (Cash) credits winnings directly to the user's available balance, while Behaviour 2 (Reinvest) divides the prize by the ticket price and rounds up to purchase new ticket entries.
- Syndicate Payouts: For group play, jackpots are split based on exact participations without prior rounding and converted to the user's local currency to guarantee no individual payout falls below \$0.01.

Game Integration Architecture

- Casino Integration: Integrated via Certified Aggregators (e.g., Oryx, Playtech) and delivered via secure IFrames, keeping the game logic on provider servers. A Seamless Wallet Protocol triggers real-time API requests to update the central balance without page refreshes.
- Lottery Integration (Messenger Model): Utilises providers to purchase official physical/digital tickets for international draws. Automated scrapers match official results against the purchased ticket DB to trigger payouts.

Payment Orchestration & The “Cascade” Engine

Routing and fee calculations are handled by the TPPS system to maximise Approval Ratios (AR) via a “Single-Pass” model.

- Routing Logic: Processors are ranked dynamically based on a 4-month rolling average AR per BIN: GOOD (>50%), AVERAGE (20%–50%), and BAD (<20%).
- Traffic Configuration (Cascade): Managed via `ttps.processor_criteria_mapping` based on country, card type, and user type.
- The 100% Rule: Assigned percentages must equal exactly 100%. Setting a processor to 0% effectively blocks specific traffic. Any modification requires a mandatory TPPS restart (Port 2012).
- Fees Handler: A microservice evaluates extra fees (10% card handling; 15% cryptocurrency volatility).

- **Processor Integration & Data Flow:** External manual gateways are strictly integrated using AES/CBC/PKCS7Padding encryption. The round-trip data exchange requires SHA-256 HMAC digital signatures placed within the x-requested-with headers. For internal real-time financial executions, the system generates an XML payload sent via sockets directly to the Java system for sequential processing.
- **Cashier Technology & FMS Integration:** The Cashier portal logic operates on the RAPI layer built in PHP 5.6–8 (Laravel), while the payment orchestration engine (TPPS) runs on Java 21 / 1.8. The Fraud Management System (FMS) relies on Maxmind minFraud for BIN enrichment and risk scoring (a score of 50+ triggers a manual alert). Adding any new fraud rule requires a mandatory Cashier recompilation.
- **Inside vs. Outside the Cashier**
 - **Inside the Cashier (Frontend):** Manual interactions pass through the Golang Wrapper RAPI (handling rate limiting and JWT validation) before entering the Cashier, where they are evaluated by the FMS and routed by the Cascade engine.
 - **Outside the Cashier (Automatic Renewals):** Subscriptions, lotteries, and memberships are handled via automated batch processing. For events like raffles, the system automatically reserves tickets with the provider first, then executes the credit card charge. If the automated charge fails, the subscription status is marked as “On Hold”.
- **Post-Confirmation Processing (Matching, Accounting & Emails)**
 - **Order Matching & Overlap Prevention:** To correctly match payments and prevent overlapping transactions, the backend identifies pending carts and securely locks them using the system_settings table.
 - **Integrity Validation:** The automated Cart Checker audits the completed transaction by validating order statuses (2, 4, 5, 7). It scans for negative prices, ensures applied discounts exactly match promotional points, and cross-references price tables to ensure financial integrity.
 - **Accounting:** All verified transactions, user updates, and fraud checks are recorded and maintained in the primary transactional database, MySQL 5.1.
 - **Customer Communication:** Once the payment is matched and reconciled, the automated mailing system dispatches HTML templates to the customer to confirm their purchase, notify them of syndicate inclusions, and provide subsequent draw results.

Payouts & Auto-Claims

- **Auto-Claims:** Unclaimed prizes from the last 40 days process automatically.
- **Winning Behavior:**
 - **Behaviour 1 (Cash):** Winnings credited directly to user balance.
 - **Behaviour 2 (Reinvest):** Prize is divided by ticket price to generate new entries, rounded up via ceil().

- Group Play (Syndicates): Jackpots are split by exact participations without prior rounding, converting to local currency to guarantee no payout is below \$0.01.
- Mexico Settlement: Finalised only when the Lotenal XML matches internal calculated records.

Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)

1. Workforce Continuity & Mobility

To prevent business paralysis in the event of physical disasters, extreme weather, or office inaccessibility:

- Universal Mobility: All staff across Engineering, Customer Support, Marketing, and Finance are equipped with corporate-configured laptops (External Information). This enables an immediate transition to a 100% remote operational model with zero loss of productivity.
- Cloud-Based Tooling: Critical operations do not rely on physical on-premise servers. The Marketing team operates through centralized SaaS platforms like Emarsys, Optimove, Looker Studio, Canva, Figma, and WordPress. Engineering and Support manage workflows and incidents remotely using Zendesk and the Atlassian suite (Jira, Confluence).

2. Core Infrastructure & Database Resilience

The platform's hybrid Hexagonal / Clean Architecture and Domain-Driven Design (DDD) allow specific modules to be isolated, scaled, or recovered independently without affecting the entire ecosystem.

- Centralized Cloud Hosting: All servers and infrastructure are hosted on AWS to guarantee scalability and disaster recovery (External Information), while infrastructure logs are securely backed up and centralized using AWS Cloudwatch.
- Database High Availability: To prevent a Single Point of Failure (SPOF), the primary transactional database (MySQL 5.1, used for orders, the Fraud Management System, and TPPS) is completely isolated from a secondary database (MySQL 5.7), which is specifically reserved to maintain the high availability of the Proxy and RAPI servers. Additionally, Memcached and Redis are used for low-latency distributed caching.

3. Domain Topology & Attack Mitigation

To prevent network outages or targeted attacks from completely halting operations, the network architecture strictly segregates domains into three contingency tiers:

- Customer-Facing Domains: Strictly used for public brands and products, such as wintrillions.com, lottoelite.com, aztecamessenger.com, and lotosena.co.
- Edge Access Domains: To ensure that a downed public domain does not cause a total system disruption, all APIs and backend services are routed through alternate domains, typically using the .io TLD (e.g., wintrillions.io, lottokings.io, legacyeight.io). If the main site crashes, the backend will continue processing automatic renewals, payments, and provider webhooks seamlessly.

- Internal Access Domains: Domains like litermi.io are reserved for internal employee interactions, strictly isolating higher production environments from lower test/stage environments.

4. Payment Engine & Financial Continuity (Cascade)

The Java-based transactional engine (TPPS Core) relies on built-in contingency mechanisms to protect revenue streams.

- Failing Processor Lockdown (The 100% Rule): If an external payment gateway experiences a massive outage, administrators can utilize the `tps.processor_criteria_mapping` table to instantly adjust the failing processor's traffic allocation to 0%. This blocks the failing route and redirects 100% of the traffic to healthy processors (requires an emergency restart of TPPS Port 2012).
- Automated Audit & Recovery (Cart Checker): During transactional interruptions, the Cart Checker module actively validates order statuses (2, 4, 5, 7) to prevent duplicate charges, correct price discrepancies, and flag abandoned carts.

5. Game Provider Contingency

- Platform Protection (Circuit Breakers): To ensure that an outage from an external Casino aggregator (like Oryx or Playtech) or a Lottery messenger provider does not cascade and crash internal servers, the system actively utilizes Resilience4j Circuit Breakers. This cuts the connection to the failing provider instantly.

6. Regulatory Compliance Resilience (KYC/AML & Fraud)

Identity verification and fraud prevention maintain continuous operations through automated fallback mechanisms:

- FMS Risk Evaluation: The system continuously evaluates risk using Maxmind minFraud; a risk score of 50 or higher triggers manual alerts to halt fraudulent transactions before they process.
- Identity Verification Contingency (Sumsub): If the silent background validation via the REST API (First-level-check-birth) fails after 3 automatic attempts due to data interruptions, the frontend immediately deploys the Sumsub WebSDK IFrame as a backup. This ensures the user has an open 30-day window to manually upload their passport and proof of address without halting the onboarding process.
- Webhook Audit Backup (MongoDB): Sumsub compliance notifications are received by a robust module built on Java 21 (Spring Boot). To prevent the loss of critical AML events if the primary MySQL database crashes, every received webhook is immediately persisted into a dedicated MongoDB database. This guarantees that compliance teams can always audit events retrospectively.

7. Crisis Management Protocols, Monitoring & Alerts

A multi-tiered alerting system ensures that Site Reliability Engineering (SRE) and operations teams can react to infrastructure emergencies in real-time:

- Centralized SRE Monitoring: Teams oversee live system metrics using Prometheus/Grafana (Micrometer) and analyze distributed logs for crashes via the ELK Stack (Kibana).

- Unified Emergency Channel (Slack): The operational status of critical providers is funneled directly into the #providers-status Slack channel via webhooks and status pages. This includes real-time notifications for AWS, Atlassian (Jira, Confluence), Mailgun, and Maxmind. (Zendesk pushes emergency status alerts exclusively via email).
- Internal Transactional Alerts: In the event of database errors, game provider API failures, or transactions getting "stuck" in the shopping cart, system administrators instantly receive automated email alerts.

8. Immediate Deployment Recovery (Zero Downtime & Rollbacks)

System deployments and updates are strictly designed to require zero operational downtime.

- Compilation & Hot-Swapping: Code is compiled using mvn clean install on JDK 1.8.
- Mandatory Live Backups for Rollbacks: Before any production deployment, protocol strictly mandates a live system backup (e.g., cp trillonario.jar trillonario.jar-\$(date +%F)). If a critical failure occurs during deployment, the team can execute an instant rollback by restoring the previous working binary and restarting Port 2012, mitigating any disruption caused by faulty code

Diagram of the technical infrastructure: Attached.

j. Critical Digital Records Storage

Regulation: The digital records maintained regarding certain critical information about players, their gaming transactions, and their financial transactions must be kept available for the CGA at all times on a server of a Tier-IV certified data centre established in Curaçao.

Current State:

A Tier-IV certified data centre facility does not currently exist within the jurisdiction of Curaçao. Consequently, the company is committed to migrating its critical storage infrastructure to a local Tier-IV facility as soon as these technical capabilities become available on the island.

Interim Technical Infrastructure

In the meantime, to ensure absolute data integrity and regulatory compliance, AWS CloudWatch is utilised to securely maintain, log, and monitor all critical player, gaming, and financial records.

Justification and System Security of AWS CloudWatch

- **Unrivalled Security and Compliance:** AWS CloudWatch operates within Amazon Web Services' infrastructure, adhering to the highest global security standards (including ISO 27001, SOC 1/2/3, and PCI-DSS). This ensures our player profiles and financial transactions are fully encrypted and shielded from unauthorized access.
- **Exceptional Reliability and Availability:** Leveraging AWS's redundant architecture guarantees that our digital records remain highly available and instantly retrievable for the CGA at all times, matching or exceeding standard Tier-IV uptime parameters.
- **Advanced Monitoring and Cost-Efficiency:** AWS CloudWatch tracks our system health and transactional events in real time. From an operational perspective, it is extremely difficult to find an alternative server or logging service that provides this elite level of safety and reliability while remaining so cost-efficient and scalable for our business volume.

C. Drommond

Legacy Eight Curaçao N.V.
eMoore N.V.
Managing Director
Signed by: Cornelia F. Drommond-Oonincx
Proxy holder eMoore N.V.
Date: 29/06/2026

