REQUERIMIENTOS TÉCNICOS DEL SISTEMA PARA LA OPERACIÓN DEL JUEGO DE SUERTE Y AZAR RIFAS

ABRIL 2025

OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN.

Tabla de contenido

GLOSARIO
OBJETIVO
CONSIDERACIONES

Contenido

GLOSARIO

1. **Anexo de requerimientos técnicos:** Normativa expedida de manera conjunta entre Coljuegos y el Consejo Nacional de Juegos de Suerte y Azar como documento maestro, donde se definen los requisitos técnicos mínimos de la infraestructura tecnológica y/o electrónica dispuesta por el operador tecnológico para la solicitud de autorización de rifas por parte de los gestores, operación del juego y para efectos de control de la operación. Los requisitos técnicos requeridos deberán ser certificados por un laboratorio de pruebas avalado por Coljuegos.

2. **Jugador o Apostador:** persona que realiza la apuesta para participar en el juego, mediante la cual constituye un contrato con el operador.

3. **Autoridades Competentes:** Son las entidades de que trata el artículo 2.7.3.3 de la Parte 7 del Libro 2 del Decreto 1068 de 2015, Único Reglamentario del Sector Hacienda y Crédito Público, en lo relativo a la modalidad de juegos de suerte y azar - RIFAS.

4. **Consejo Nacional de Juegos de Suerte y Azar (CNJSA):** es un organismo administrativo que pertenece a la Rama Ejecutiva del Sector Central, adscrito al Ministerio de Hacienda y Crédito Público. Entre sus funciones se encuentran la de aprobar y expedir los reglamentos y sus modificaciones de las distintas modalidades de juegos de suerte y azar, cuya explotación corresponda a las entidades territoriales y vigilar el cumplimiento de la Ley 643 de 2001 y de los reglamentos de las distintas modalidades de juegos de suerte y azar, cuya explotación corresponda a las entidades territoriales**.**

5. **Coljuegos:** Empresa Industrial y Comercial del Estado Administradora del Monopolio Rentístico de los Juegos de Suerte y Azar -COLJUEGOS.

6. **Escrutinio:** Proceso técnico, sistemático y controlado mediante el cual se validan, consolidan y verifican las apuestas registradas en las rifas, confrontándolas con los resultados oficiales de las loterías autorizadas o los resultados del GNA para determinar las combinaciones ganadoras y, por ende, las apuestas que tienen derecho a reclamar un premio.

7. **Rifa:** *"La rifa es una modalidad de juego de suerte y azar mediante la cual se sortean en una fecha predeterminada, premios en especie entre quienes hubieren adquirido o fueren poseedores de una o varias boletas emitidas con numeración en serie continua y puestas en*

venta en el mercado a precio fijo por un operador previa y debidamente autorizado." Artículo 27 de la Ley 643 de 2001.

8. **Gestor:** *"Es la persona natural o jurídica interesada en la realización, organización, comercialización y promoción del juego de suerte y azar en la modalidad de rifas autorizadas a través del operador y que podrán ofrecer de manera física o electrónica a través de una plataforma web o de redes sociales."* Decreto 1486 del 2024.

9. **Cadena de bloques (blockchain, en inglés):** Tecnología que permite disponer de una base de datos distribuida y descentralizada formada por cadenas de bloques diseñadas para evitar su modificación una vez que un dato ha sido publicado; se utiliza un sello de tiempo confiable y se enlaza a un bloque anterior, permitiendo la transferencia de activos y datos de manera comprobable y confiable.

10. **Canal de comercialización por internet:** sitio en internet que permite habilitar las ventas de juego de suerte y azar RIFAS de forma segura, que por medio de Dispositivos de Conexión Remota (DCR) a través de canales interactivos que permitan al Software de Gestión de Rifas - SGR - recibir toda la información correspondiente a las apuestas de un jugador y generar boletos electrónicos, así como la consulta de sorteos realizados.

11. **Certificado SSL:** Un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.

12. **Código fuente:** Es un conjunto de líneas de texto con instrucciones, escritas en un lenguaje de programación, que guían el proceso de ejecución de un programa. Estas instrucciones, que son comprensibles para humanos, están redactadas por un programador.

13. **Código único de seguridad:** Código hash que respalda la información contenida en el boleto mediante la implementación del algoritmo de seguridad criptográfica SHA-256.

14. **Dispositivos de Conexión Remota (DCR):** Diferentes artefactos que permiten conexión a distancia, en línea y tiempo real con el Sistema Central del Juego como un canal adicional de venta, validación del boleto y promoción del juego.

15. **En línea:** Expresión que se utiliza para denotar que un elemento se encuentra conectado o hace parte en forma permanente de un sistema de información. La operación en línea

implica, además, que los programas se ejecutan de tal forma que los datos se actualizan de inmediato en la o las bases de datos del sistema.

16. **En tiempo real**: Expresión que se utiliza en los sistemas informáticos para indicar que tienen capacidad de sincronizar en intervalos de tiempo bien definidos, el funcionamiento del sistema en simultánea con las acciones que se presentan en el mundo físico. Requisito obligatorio para la operación de los juegos de suerte y azar en Colombia.

17. **Firma digital:** Mecanismo criptográfico que asegura la autenticidad, integridad y no repudio de un mensaje o documento electrónico. Funciona mediante un esquema de criptografía asimétrica, donde el remitente utiliza una clave privada para cifrar un hash del documento, creando la firma, y el receptor verifica su validez con la clave pública del remitente. Esto garantiza que el documento proviene de una fuente legítima y no ha sido modificado.

18. **Número aleatorio:** es un número obtenido al azar, es decir, que todo número tiene la misma probabilidad de ser elegido y que la elección de uno no depende de la escogencia del otro.

19. **Generador de Número Aleatorio (GNA):** Sistema hardware y/o software que produce secuencias de números estadísticamente independientes e impredecibles, que definirá el resultado de los sorteos del juego y/o apuestas automáticas.

20. **Información de control:** Eventos significativos o sucesos generados en las terminales de venta que se utilizan para realizar control a la operación. Ejemplos: apuesta anulada, y reseteo de la terminal de venta o apuestas realizadas por internet.

21. **Interfaz de comunicaciones:** Dispositivo electrónico o componente de software que permite la comunicación entre las Terminales de Venta y el Sistema Central del Juego.

22. **Internet:** Red de comunicación interconectada que puede ser usada como un canal adicional de venta y promoción del juego a través de una página web o aplicación de dispositivo móvil.

23. **Red de comunicaciones:** Elementos que garantizan la comunicación confiable y oportuna entre los diferentes componentes que conforman el SCJ, y por las terminales de venta, dispositivos de conexión remota e internet, para asegurar la adecuada operación y continuidad del juego.

24. **ISO/IEC 27001:** Creado por la International Organization for Standardization y la International Electrotechnical Commission, es un estándar para la seguridad de la

información, que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de seguridad de la información.

25. **Latencia de red:** Es el retraso en la comunicación de la red. Muestra el tiempo que tardan los datos en transferirse a través de la red. Las redes con un mayor retraso o retardo tienen una latencia alta, mientras que las que tienen tiempos de respuesta rápidos tienen una baja.

26. **Plataformas digitales:** Las plataformas digitales o plataformas virtuales, son espacios en Internet que permiten la ejecución de diversas aplicaciones o programas en un mismo lugar para satisfacer distintas necesidades. Entre estas tenemos los canales públicos a través de internet.

27. **PCI – DSS:** Por sus siglas en inglés Payment Card Industry Data Security Standard, es un estándar de seguridad de datos definido para la industria de tarjetas de pago.

28. **Protocolo de comunicaciones:** Conjunto de reglas normalizadas que permiten el intercambio de información entre equipos informáticos, así como posibles métodos de recuperación de errores.

29. **Proveedor de servicios de comunicaciones:** Persona jurídica responsable de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros.

30. **Punto de venta:** Lugar físico donde se podrá realizar la compra de boletas a través de terminales de venta y consultar resultados.

31. **Red de comunicaciones:** Elementos que garantizan la comunicación confiable y oportuna entre los diferentes componentes que conforman la plataforma tecnológica del juego, y por los terminales de venta para asegurar la adecuada operación y continuidad del juego.

32. **Sistema Central del Juego - SCJ -:** Plataforma tecnológica que soporta el juego la cual está compuesta por los elementos de hardware requeridos y el conjunto de programas (software) que garantizan la adecuada operación del juego: Software de Gestión de RIFAS, Software de Validación de Apuestas, Software de Generación de Sorteos, Software de capa media y Hardware de Almacenamiento. Los elementos básicos del sistema central de juego son definidos dentro de los Requerimientos Técnicos aprobados mediante normativa expedida de manera conjunta entre Coljuegos y el Consejo Nacional de Juegos de Suerte y Azar.

33. **Software de Gestión de RIFAS - SGR:** Software o plataforma tecnológica encargada de llevar el registro, la autorización y el control de gestores, gestionar el proceso de autorización, la operación, el flujo financiero y los procesos de vigilancia y control de las Rifas

34. **Software de Validación de Apuestas:** Software donde se reciben, validan, procesan y almacenan las apuestas que se realizan en los diferentes terminales de venta.

35. **Software de generación de sorteos:** Software que por medio de un Generador de Números Aleatorios - GNA - realiza la selección de los números para determinar la combinación ganadora del juego.

36. **Software de capa media y Hardware de Almacenamiento**: Conjunto de elementos necesarios para garantizar el correcto almacenamiento de la información tales como servidores, bases de datos, y sistemas de respaldo, entre otros.

37. **Streaming:** Es una tecnología de transmisión de audio y video (mientras sucede), entregado para su visualización en línea y tiempo real a computadoras o cualquier otro dispositivo conectado a internet.

38. **Terminal de venta TDV:** Dispositivo fijo o móvil que permite registrar las apuestas que requiera el jugador para participar en las rifas. Este dispositivo se encuentra conectado en línea y en tiempo real con el Sistema Central del Juego.

39. **TIER III:** Por su sigla en inglés "*Telecomunications Infraestructure Standard for Data Centers*" corresponde al nivel de fiabilidad que debe tener un centro de cómputo de acuerdo con las características del negocio. Existen cuatro niveles de Tier donde a mayor número, mayor disponibilidad tendrá el centro de cómputo. Tier III opera con una disponibilidad del 99.982%, lo que significa que la infraestructura garantiza que el sistema no fallará más de 1.57 horas al año y que no habrá interrupciones por mantenimientos planificados.

40. **Topología de Red:** Se define como el mapa físico o lógico de todos los componentes utilizados para intercambio de datos en una red. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados"

41. **VPN:** Tecnología de comunicaciones que permite la conexión entre dos sitios para el intercambio de información. Se conoce como VPN por las siglas en inglés de "Virtual Private Network".

42. **El código QR "Respuesta Rápida" (Del inglés Quick Response code):** Es un tipo de código de barras bidimensional capaz de almacenar determinado tipo de información, como una URL, SMS, e-mail, texto, etc. Y permite, al ser escaneado ver la información que contiene.

43. **Nube pública:** Es un modelo de computación en la nube en el cual los recursos, tales como servidores, almacenamiento y aplicaciones, son proporcionados por un proveedor externo a través de internet. Estos recursos son accesibles para múltiples usuarios o entidades, que comparten la misma infraestructura. La nube pública ofrece ventajas como escalabilidad, flexibilidad y disponibilidad del 99.999%, al permitir a los usuarios ajustar el uso de los recursos según sus necesidades sin la necesidad de gestionar ni mantener infraestructura física propia.

44. **Georreferenciación:** Es la asignación de coordenadas geográficas a datos o elementos, permitiendo su ubicación precisa en un mapa o sistema de información geográfica (SIG) para su análisis y visualización en el espacio.

45. **Contrato Inteligente (En Inglés - Smart Contract):** Programa informático que se ejecuta de manera automática en un Blockchain sin necesidad de intermediarios.

46. **Operador:** "*Persona jurídica autorizada en Colombia por las autoridades competentes para operar el juego de suerte y azar en la modalidad de Rifas, para lo cual se debe dar cumplimiento a las obligaciones fijadas por la ley, en el presente reglamento, en los Requerimientos Técnicos para la operación del Juego que expidan la Empresa Industrial y Comercial del Estado COLJUEGOS, en la autorización de operación otorgada y demás normas que las modifiquen, sustituyan o adicionen. El operador coordinará a los gestores de rifas y será el responsable de liquidar y garantizar el recaudo de los gastos de administración, derechos de explotación y cualquier otra renta y/o tarifa que se genere por la operación del juego, recursos que deberán ser transferidos en los términos y condiciones establecidos en la normativa vigente. El operador aportará toda la infraestructura operativa, tecnológica y/o electrónica requerida para presentar ante el competente la solicitud de autorización de las rifas a realizar por los gestores, y para la operación del juego, la cual deberá ponerla al servicio de la autoridad competente para efectos de control de la operación"*. Decreto 1486 del 2024.

47. **Plataformas digitales**: son espacios en Internet que permiten la ejecución de diversas aplicaciones o programas en un mismo lugar para satisfacer distintas necesidades.

48. **Plataformas de streaming en vivo:** Es un servicio que difunde la información de audio/video en tiempo real. El reproductor del ordenador del visitante interpreta esta transmisión y la visualiza inmediatamente. Tal tecnología requiere servidores dedicados potentes porque necesita gran cantidad de recursos para que funcione correctamente. Existen numerosas plataformas dedicadas al streaming, como: YouTube Live, Twitch, Kick, Instagram y Facebook Live.

CONSIDERACIONES

Coljuegos y el Consejo Nacional de Juegos de Suerte y Azar reservan todas las facultades para definir el detalle de los procedimientos, requisitos y condiciones técnicas que, por su misma naturaleza, puedan estar sujetos a cambios derivados de la innovación tecnológica.

En la elaboración de este documento se ha considerado la normativa, estándares internacionales y reglamentaciones técnicas, así como el Decreto 1486 del 2024.

El cumplimiento de los requerimientos técnicos del juego de suerte y azar RIFAS, incluidos en el presente documento así como los anexos que hagan parte integral de la solución tecnológica, deberán certificarse por los laboratorios avalados por COLJUEGOS.
Es importante señalar que las disposiciones establecidas en este documento se basan en el Decreto 1486 de 2024 vigente al momento de su redacción. Sin embargo, dado que la normativa aplicable puede sufrir modificaciones o actualizaciones en el futuro, se reconoce que ciertos requisitos o procesos podrían ajustarse para cumplir con las nuevas regulaciones emitidas por las autoridades competentes. El Operador deberá garantizar que sus sistemas y procedimientos se mantienen conformes a la normatividad vigente.

Para efectos de determinar la competencia para la autorización de rifas, se remite a lo dispuesto en el artículo 2.7.3.3. Del Decreto 1068 de 2015, del cual se extraer e indica lo siguiente:

Jurisdicción de la Rifa	Entidad Administradora del Monopolio
Operación únicamente en un (1) municipio de un departamento.	Alcaldía
Operación únicamente en el Distrito Capital	Lotería de Bogotá
Operación en dos (2) o más municipios del mismo departamento. Operación en un (1) municipio de un departamento y en el Distrito Capital.	Sociedad de Capital Público Departamental
Operación en dos (2) o más municipios de diferentes departamentos. Operación en dos (2) o más municipios del mismo departamento y el distrito capital.	Coljuegos

Es importante que el Operador autorizado realice una integración de su SGR con el *software* plataforma electrónica web o sistema informático que realizará el sorteo mediante un GNA tal como se especifica en este documento, lo anterior, permitiendo a la autoridad competente hacer el respectivo seguimiento, control y verificación de la veracidad y transparencia del sorteo como

el seguimiento a la comercialización de la rifa. De igual modo, se debe integrar el nombre de la lotería tradicional o billetes contra el cual se realizará el sorteo. Este requisito no aplica para la comercialización de rifas con boletas físicas y comercialización manual.

Por otro lado, la presentación de la solicitud de autorización deberá realizarse 30 días antes de la fecha del sorteo de acuerdo al cumplimiento de requisitos definidos en el Decreto 1486 del 2024.

OBJETIVO

El presente documento define las especificaciones técnicas que son esenciales para la operación del juego de suerte y azar RIFAS. Este marco técnico establece los parámetros que deben cumplir las plataformas tecnológicas dispuestas por los operadores tecnológicos, garantizando el cumplimiento de las normativas, la transparencia y la seguridad del juego acorde a lo dispuesto en el Decreto 1486 del 2024 que modifica el Decreto 1068 del 2015.

1. ASPECTOS TÉCNICOS GENERALES

El sistema técnico de juego y en general el conjunto de sistemas e instrumentos tecnológicos, que posibiliten la organización, comercialización y celebración del juego de suerte y azar RIFAS, debe disponer de los mecanismos de autenticación suficientes para garantizar, entre otros, la continuidad del juego, confidencialidad e integridad en las comunicaciones, validación, autenticidad y cómputo de las apuestas, el control de su correcto funcionamiento y el acceso a los componentes del sistema informático exclusivamente del personal autorizado de las Autoridades Competentes en las condiciones que este pudiera establecer.

El operador tecnológico debe disponer de la plataforma necesaria para el desarrollo de las actividades del juego debidamente certificados por un laboratorio avalado previamente por Coljuegos, correspondiendo al operador tecnológico la certificación del Sistema Central de Juego.

El sistema Central de Juego empleado por el operador tecnológico y el desarrollo de las actividades de juego por medios electrónicos, informáticos, telemáticos e interactivos, deben reunir las condiciones técnicas contenidas en este documento.

La infraestructura tecnológica dispuesta por el operador tecnológico, se encuentra compuesto por el Sistema Central del Juego – en adelante SCJ, la red de comunicaciones, dispositivos de conexión remota – en adelante DCR, las Terminales de Venta – en adelante TDV, el Software de Generación de Sorteos – en adelante GNA, además del Software de Gestión de RIFAS - en

adelante SGR. Este SCJ debe disponer de los mecanismos de autenticación suficientes para garantizar, entre otros, la ubicación, la identificación y autenticación digital de las TDV, o de los DCR a través de los cuales se conectan los jugadores si es por internet. Además, debe garantizar la confidencialidad e integridad en las comunicaciones y el seguro almacenamiento de la información del juego y del apostador.

El siguiente diagrama muestra en forma genérica su arquitectura:

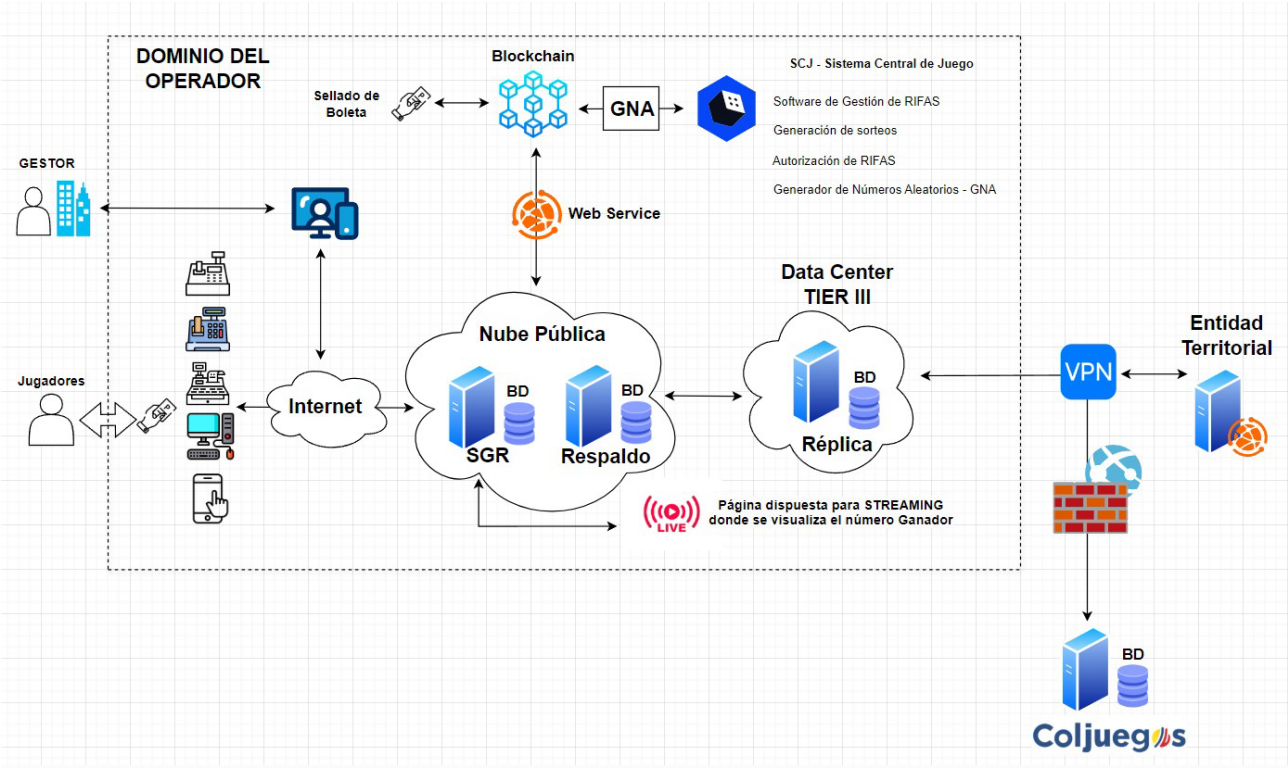


Ilustración 1. Fuente: Coljuegos.

Las Autoridades Competentes y en CNJSA, podrán acceder al Data Center TIER III mediante VPN para consultar toda la información que el Operador tecnológico debe reportar para efectos de seguimiento y auditoría del juego. Es importante resaltar que, en el Data Center TIER III no se debe tener un SGR adicional a los ya existentes en la nube pública, solo se debe contar con la base de datos en la réplica. Esta base de datos en la réplica, será una copia íntegra, completa y en su totalidad de la base de datos que exista del SGR y no únicamente de las transacciones que se realicen como resultado de las actividades del SGR. Lo anterior, permitirá a las Autoridades Competentes y de vigilancia acceder completamente a toda la información y logs, que se encuentren almacenados en la base de datos del SGR y que se replican en el Data Center TIER III en la base de datos dispuesta para tal fin. Esto con el propósito de no interferir en la base de datos de producción del SGR.

El SGR y su respaldo (contingencia) deberán estar en nubes públicas. El respaldo puede estar en la misma nube pública que el SGR, o en una nube pública diferente. La réplica deberá permanecer ubicada en un data center con características mínimas de TIER III o superior en territorio colombiano. Cabe aclarar que, tanto la Autoridad Competente como el Consejo Nacional de Juegos de Suerte y Azar, podrán acceder a la base de datos de la réplica como a la base de datos del SGR y su respaldo mediante una VPN y cuando la Autoridad Competente y el Consejo Nacional de Juegos de Suerte y Azar lo disponga.

En ningún caso el SGR, el respaldo y la réplica de información al que accede la Autoridad Competente y la de vigilancia, estarán en un centro de cómputo de propiedad de la autoridad competente o la de vigilancia, en consecuencia la administración, gestión, actualización, costos y análisis de riesgos, entre otros y sin limitar a, serán de responsabilidad del operador tecnológico.

El SCJ deberá ser provisto, instalado, puesto en operación, licenciado, administrado y soportado por el Operador tecnológico y deberá cumplir con las siguientes especificaciones:

. Una infraestructura que contenga el Software de Gestión de RIFAS - SGR con su respectiva base de datos de la réplica.

  Este sistema debe tener como mínimo las siguientes características:

  - Frontend en ambiente web.
  - Módulo de administración de usuarios.
  - Módulo de autorización y operación.
  - Módulo de reportes financieros, de ventas, de novedades, de premios, estadísticas, escrutinio, entre otros y que permita la generación de reportes con las múltiples combinaciones de datos disponibles.
  - Todo el licenciamiento a nivel de los diferentes componentes de software requeridos, independiente del usado para el SCJ.

b. Base de datos en motor SQL Server última versión estable y actualizable con capacidad suficiente de almacenamiento para los datos históricos de la operación durante la vigencia de la acreditación como operador tecnológico y dos años más. Se debe tener en cuenta la necesidad de sistemas Master-Slave (Maestro-Esclavo) en la solución en caso que así

se requiera para la réplica, esto con el fin de tener siempre una copia íntegra de toda la base de datos del SGR.

De esta base de datos se debe incluir:

- Diccionario de datos de todas las tablas que componen la estructura de la base de datos.
- Diagrama entidad-relación y modelo relacional.
- Toda la documentación relacionada con los objetos de la base de datos.
- El modelo de datos que forma parte integral del presente anexo de requerimientos técnicos.
- Todo el licenciamiento a nivel de los diferentes componentes de software requeridos, independiente del usado para el Sistema Central del Juego.
- Se debe garantizar, la integridad de la información almacenada en la o las bases de datos y sistemas de información, mediante el uso de herramientas que cumplan con dicha función y garanticen el cumplimiento de controles automáticos en dichos entornos (a modo de ejemplo y sin limitar a: IBM Guardium, Data Activity Monitor). Igualmente, la implementación de logs de auditoría en bases de datos, entre otros controles aplicables, que garanticen la trazabilidad de los cambios de un dato generado durante el tiempo. Las Autoridades Competentes y de vigilancia deberán contar con los diferentes accesos a dichas herramientas que evidencien el comportamiento de los datos a lo largo del tiempo. Será responsabilidad del operador la implementación y gestión de dichos controles con la herramienta que se ajuste a su solución tecnológica.

c. Todo el software instalado y suministrado en las máquinas, incluyendo y sin limitar a: sistemas operativos, bases de datos, software capa media, aplicaciones de negocio, software antivirus, software de cortafuegos y/o cualquier aplicación que se requiera para el funcionamiento de la solución debe estar debidamente ***licenciado*** y contar con la opción de actualización a la última versión disponible en el mercado por el periodo acreditación como Operador Tecnológico. Se requiere la entrega de los debidos soportes.

d. Entrega ***manuales*** del sistema, de instalación, y de usuario y toda aquella documentación, entre otra y sin limitar a: diagramas físicos (a modo de ejemplo:

componentes, microservicios, etc.) y lógicos (a modo de ejemplo: casos de usos, clases, etc.), configuraciones, parametrizaciones, manuales de resolución de fallas, los cuales serán objeto de verificación en producción y de actualización mínima una vez durante cada año de acreditación o cuando surjan cambios o modificaciones en el SCJ.

e. En caso de fallas en los medios de comunicación o en alguno de los extremos, se debe contar con los ***servicios de sincronización*** que se requieran para garantizar que toda la información repose en los contenedores de la base de datos a las que acceden las Autoridades Competentes y de vigilancia.

f. El o los medios de comunicaciones, debe contar con características de ***cifrado*** AES-256 (en modo GCM o CTR), o superior, que permita la sincronización de la información en línea y en tiempo real y contar con una ***disponibilidad*** garantizada del 99.982% buscando siempre un respaldo sobre una arquitectura robusta, redundante y diseñada específicamente para evitar puntos únicos de fallo. Las especificaciones técnicas de estos medios de comunicación se deben ajustar a las necesidades reales de operación que sean requeridas, las mismas deben ser ajustadas de acuerdo a la demanda, la velocidad, disponibilidad, seguridad y confiabilidad de la solución, sin que este elemento se constituya en un cuello de botella que impida el normal funcionamiento de la solución. Dichos elementos de comunicación deben permitir la trasmisión de información en línea y en tiempo real.

g. Se deben incluir todos los ***elementos requeridos*** para la implementación y operación de la solución de replicación. En caso que el servicio contratado con el Data Center TIER III sea a modo de "Colocation o Server Homing", se debe garantizar la inclusión y sin limitar a: cableados estructurado, eléctrico, fibra óptica, instalación de protecciones eléctricas, posible uso de PDUS en el rack del centro de cómputo, canalizaciones, obras civiles, mediciones y ajustes de la red eléctrica y en general todo dispositivo o servicio requerido para la normal operación de la solución.

h. Se debe incluir la ***ejecución de tareas realizadas*** para, sin limitar a: configuración a nivel de hardware y software, tuning o afinamiento de sistemas operativos y bases de datos, pruebas de stress, hardening, pruebas de calidad, pruebas de integridad, pruebas de sincronización, pruebas de trasmisión de datos de la solución, entre otras.

i. Toda la solución suministrada, incluyendo todos los componentes de hardware y software deben ser ***IPv6*** Compatible, permitiendo la configuración de ambientes nativos en IPv6

y Dual Stack IPv4 / IPv6. En caso de ser requerido, se debe anexar las certificaciones de los fabricantes que avalen dicha condición de operación.

j. Se debe incluir todas las ***soluciones de software***, capa media, seguridad de la información (firewall), elementos de autenticación, sistemas de asignación de direcciones, autenticación de dominio, conversores y en general todos los elementos de software requeridos para la normal operación integral de la réplica. Lo anterior, debe permitir la visualización de la información incluida en la Base de Datos, así como los tableros de control, reportes y Dashboard solicitados al operador tecnológico como parte del sistema de información.

La administración, el funcionamiento, cumplimiento de normas, estándares y reglamentaciones técnicas de la plataforma tecnológica, será responsabilidad del Operador tecnológico autorizado por las Autoridades Competentes, quien dispondrá directa o indirectamente, pero siempre bajo su responsabilidad, por la red de comunicaciones, el software, equipos, sistemas, terminales de venta e instrumentos en general necesarios para garantizar el funcionamiento del sistema.

El Operador deberá asegurar que, en línea y en tiempo real, se replique en el Data Center TIER III la totalidad de la base de datos que exista del SGR de manera íntegra y completa y no únicamente de las transacciones que se realicen como resultado de las actividades del SGR. Asimismo, a partir de la información detallada de las apuestas generadas en las TDV o por internet, los resultados de los sorteos y los pagos de premios almacenados, el SGR será responsable de generar la información administrativa y de estadísticas requeridas por las Autoridades Competentes y de vigilancia.

En el entendido que el operador tecnológico es el único responsable de la implementación, gestión, administración, entre otras responsabilidades y sin limitar a, de la réplica disponible para las Autoridades Competentes y de vigilancia, será únicamente Coljuegos la autoridad competente para aprobar o solicitar cualquier cambio, ajuste, actualización y/o intervención física o lógica a dicha réplica.

2. REQUISITOS TECNOLÓGICOS DE FUNCIONALIDAD DEL SCJ.

El SCJ debe contar con una infraestructura tecnológica estable y redundante que garantice la disponibilidad, integridad y confiabilidad de la información almacenada en la base de datos, información de control, resultados de los sorteos, información de las apuestas generadas en los TDV o jugadores desde internet por los DCR e información de los gestores.

Debe incluir todas las rutinas, controles, procedimientos y buenas prácticas en la industria, tales como políticas de backups, políticas de retención de información, políticas de despliegue, gestión del cambio y cualquier otra que le permitan ofrecer la alta disponibilidad de la plataforma.

Los componentes de la solución SCJ deben contar con una disponibilidad mínima del 99.982%, contar con planes de contingencia y redundancia que aseguren la transmisión de la información en tiempo real.

El SCJ debe permitir:

- Que la base de datos de la réplica sea una copia íntegra, completa y en su totalidad de la base de datos que exista del SGR y no únicamente de las transacciones que se realicen como resultado de las actividades del SGR.

- Controlar el correcto funcionamiento de los diferentes componentes tecnológicos que garantizan la operación del juego.

- Garantizar la integridad de la información almacenada en la o las bases de datos y SCJ, mediante el uso de herramientas que cumplan con dicha función y garanticen el cumplimiento de controles automáticos en dichos entornos (a modo de ejemplo y sin limitar a: IBM Guardium Data Activity Monitor), igualmente la implementación de logs de auditoría en bases de datos, entre otros controles aplicables, que garanticen la trazabilidad de los cambios de un dato generado durante el tiempo. Las Autoridades Competentes y de vigilancia deberán contar con los diferentes accesos a dichas herramientas que evidencien el comportamiento de los datos a lo largo del tiempo. Será responsabilidad del operador tecnológico la implementación y gestión de dichos controles con la herramienta que se ajuste a su solución tecnológica.

- Que por medio del Operador tecnológico el acceso para las Autoridades Competentes y de vigilancia a los componentes de la réplica para realizar inspección, con independencia del lugar de su ubicación y del personal que preste servicios en las instalaciones donde se encuentre alojada. En caso que el servicio contratado con el Data Center TIER III sea a modo de "Colocation o Server Homing", se debe garantizar la revisión en sitio y sin limitar a: cableados estructurado, eléctrico, fibra óptica, instalación de protecciones eléctricas, posible uso de PDUS en el rack del centro de cómputo, canalizaciones, obras civiles, mediciones y ajustes de la red eléctrica y en general todo dispositivo o servicio requerido para la normal operación de la solución. Para esta réplica, la cual debe estar en territorio nacional, el Operador será responsable de la falta de colaboración del

personal citado, además de disponer el respectivo personal técnico competente para la revisión y atención de inspecciones en los horarios establecidos por la entidad.

- Que por medio del Operador tecnológico el acceso para las Autoridades Competentes y de vigilancia a los componentes del SCJ para realizar inspección. Para el caso de la implementación en nubes públicas fuera de Colombia, los accesos deberán ser entregados a las Autoridades Competentes y de vigilancia. El Operador Tecnológico debe garantizar el acceso a todas y cada una de las herramientas, productos, dispositivos y demás con un usuario administrador con el fin de poder hacer las revisiones que sean requeridas.

- Interconectar múltiples TDV y jugadores desde internet por los DCR.

El SGR debe permitir:

- Registrar todas las transacciones y operaciones de juego realizadas desde las TDV o aquellos jugadores que desde internet utilicen DCR: Sorteos, Apuestas por sorteo, pago de premios, datos de control, así como eventos de funcionamiento del juego.

- Generar reportes administrativos de la operación del juego, incluyendo operación y premios.

- Conservar la trazabilidad del trámite general de gestión de las rifas, con estados, tiempos y actores que intervienen en el proceso.

- Contar con un módulo de búsqueda dentro del SGR.

- Contar con un módulo de mensajes informativos y/o recordatorios que mostrarán avisos, alertas y comunicaciones al respecto del proceso de autorización y operación de las rifas.

- Parametrizar las reglas de negocio básicas para la operación general del sistema, tales como: perfiles, usuarios, sorteos y apuestas.

- Registrar las transacciones financieras que se generan durante la operación para el cálculo de las ventas, sorteos y entrega de premios durante un rango de tiempo.

- Registrar todos los premios en línea, mediante conexión de los TDV o jugadores desde internet por los DCR.

- Recibir la compra de las boletas hasta 1 día hábil anterior a la hora definida por el operador para el comienzo del sorteo. Así las cosas, se deben bloquear las ventas y

anulaciones en todos los canales de comercialización. Además, el operador debe enviar el reporte de la boletería vendida y no vendida a más tardar el día hábil anterior al sorteo. El día del sorteo no se podrán comercializar más boletas.

- Realizar sorteos por medio de un GNA con Smart Contract, registrar y publicar en línea y tiempo real las combinaciones ganadoras, en los monitores y/o plataformas dispuestas para la transmisión del sorteo vía Streaming (para el caso cuando esta tecnología sea usada para la transmisión) con el aviso indicando que no se recibirán más apuestas. La cantidad y frecuencia de los sorteos está definida en el reglamento del juego o en la reglamentación vigente.

- Asegurar la existencia de información diaria y mensual para control contable de las TDV e Internet.

- Verificar en línea y tiempo real el detalle de la información de control y de las apuestas de cada uno de los TDV e Internet.

- Mantener un log de las transacciones realizadas y eventos ocurridos en las bases de datos y enviar mensualmente un reporte con los resultados y garantizar el acceso directo a las autoridades Competentes y de vigilancia.

- Proteger mediante software licenciado contra tráfico malicioso y virus informáticos todo el hardware que utilice un sistema operativo o software susceptible a infecciones.

- Gestión interna de soporte y recuperación del sistema de datos asegurando la disponibilidad del sistema.

- Generar la información de sorteos y apuestas, con corte en el cierre de operación para el reporte automático de resultados por punto de venta, TDV, Internet y ubicación geográfica (municipio).

- Registrar el pago de premios por TDV y ubicación geográfica (municipio: Latitud y Longitud).

- Implementar un control de versiones de los programas, archivos, tablas, repositorios, configuraciones, etc.

Falla en el funcionamiento: Las ventas quedarán suspendidas cuando el SCJ presente fallas en el funcionamiento ya sea por software, el hardware donde está instalado o la conectividad del mismo.

Detección de errores: El software debe estar en la capacidad de detectar cualquier falla, generar un mensaje de error como consecuencia de esta y reportar inmediatamente a las autoridades competentes mediante correo electrónico.

2.1. SISTEMA DE CONTROL PARA ALTOS FLUJOS DE TRANSACCIONES

Para garantizar la estabilidad y disponibilidad del sistema durante momentos de alta demanda en las ventas de las boletas, el SGR debe contar con un sistema de gestión y control para altos flujos de transacciones permitiendo manejar de forma automática y eficiente los picos de tráfico al momento de hacer compras de boletas en el SGR. Este sistema debe cumplir con el control de sobrecarga, manejo de prioridades en la venta de boletas, tiempo de espera, notificación a usuarios de la plataforma, escalabilidad en caso de flujos extremos de carga transaccional, persistencia y recuperación de datos, control de transacciones en espera y monitoreo en tiempo real.

2.2. TRANSMISIÓN DE SORTEOS MEDIANTE USO DE HERRAMIENTAS TECNOLÓGICAS-STREAMING.

El streaming permite interactuar con contenido multimedia sin necesidad de descargar archivos que ocupen espacio en su dispositivo. Esta tecnología envía y recibe datos en un flujo continuo a través de una red, desde un servidor remoto hasta un dispositivo. Cuando se transmiten los contenidos por internet, el DCR inicia la recepción de datos dando inicio a la visualización del contenido. Mientras éste contenido de video o audio sigue reproduciéndose, el resto de los datos se transmiten al dispositivo de forma gradual, permitiendo consumir contenidos al instante, sin tener que esperar a descargar todo el archivo.

La transmisión de los sorteos realizados con GNA se deberá realizar en tiempo real en la fecha y hora señalada en el acto administrativo de autorización expedido por la autoridad competente, garantizando el libre acceso de los interesados a la visualización.

La transmisión de los sorteos realizados con GNA deberá realizarse usando la tecnología de transmisión Streaming para cualquier Web compatible con dispositivos móviles (iOS, Android, Windows, Linux, MacOS y otros). Esta transmisión deberá ser distribuida a través de un

proveedor de servicio de streaming que garantice la total escalabilidad de la señal con el fin de evitar saturación en el servicio y retrasos en la transmisión.

Las condiciones técnicas mínimas de transmisión de servicio con tecnología streaming deberán cumplir con las siguientes especificaciones:

a) Deberá ser web y compatible con dispositivos móviles (iOS, Android, Windows, Linux, Mac OS y otros).

b) El transporte de la señal de Streaming deberá ser por canal de Internet dedicado desde el lugar de realización del sorteo o desde el software de generación de sorteo para los casos que aplique el GNA con Smart Contract, hasta el centro de distribución del Streaming.

c) Deberá contar además con alternativas de conexión con otros servicios de Internet gestionados por el operador. Como son: Internet por fibra óptica y contar como mínimo 40 Mbps dedicados.

d) Deberá contar con un canal de Streaming alterno para realizar pruebas.

e) La transmisión por redes sociales deberá contar con varias cuentas, con un mínimo de (2) dos simultáneamente como: Facebook, X, YouTube, Twitch, Vimeo, Instagram, Kick, entre otros.

f) La portada de la transmisión debe contar como mínimo la colocación de una imagen de fondo, título y descripción del sorteo de conocimiento de los usuarios.

g) Deberá contar con estadísticas que permitan conocer los usuarios conectados en vivo por tipo de dispositivo, reporte de usuarios únicos, Reporte de usuarios conectados y ubicación geográfica.

h) La plataforma debe garantizar la transmisión sincronizada de audio y video.

3. GESTIÓN DE LAS RIFAS

3.1. ROLES EN EL PROCESO

A continuación se relacionan los roles que intervienen en el proceso de gestión de las rifas.

- **Operador tecnológico.**
- **Autoridad Competente.**

- **Gestor.**
- **Apostador.**
- **CNJSA.**

3.2. REGISTRO DE GESTORES

La plataforma del Operador tecnológico dispondrá de un mecanismo de registro de gestores, mediante el cual se ingresarán todos los campos y documentos requeridos. Si la solicitud de registro no incluye la información completa, el gestor no podrá continuar con el proceso de creación de su usuario. En caso de registro exitoso, la plataforma informará al gestor que su registro ha sido completado correctamente.

Los campos y documentos a suministrar son:

Persona Natural:

- Nombre Completo.
- Tipo de documento de identidad.
- Número de documento de identidad.
- Número de teléfono de contacto.
- Correo electrónico de contacto.
- Domicilio del gestor.

Persona Jurídica:

- Razón social de la persona jurídica.
- NIT
- Certificado de Existencia y Representación Legal, expedido por la correspondiente Cámara de Comercio con fecha de expedición no superior a 30 días
- Nombre completo del representante legal
- Tipo de documento de identidad.
- Número de documento de identidad.
- Fotocopia de documento de identidad.
- Número de teléfono de contacto de la persona jurídica.
- Correo electrónico de contacto de la persona jurídica.
- Domicilio del gestor.

Cabe resaltar que los campos y documentos señalados anteriormente, se encuentran sujetos a los cambios, actualizaciones, modificaciones y peticiones adicionales que sean de consideración de las Autoridades Competentes de acuerdo con la normativa vigente.

Para el registro de un gestor, el Operador Tecnológico debe garantizar que la captura, almacenamiento y tratamiento de datos personales cumpla con la Ley 1581 de 2012, sus decretos reglamentarios, o normas que las complementen, sustituyan o modifiquen.

3.3. SOFTWARE DE GESTIÓN DE RIFAS (CREACIÓN Y AUTORIZACIÓN)

El operador deberá disponer de un software de gestión de rifas, que por medio de módulos tenga la capacidad de validar paso a paso lo correspondiente al proceso de autorización y operación de una rifa. Así las cosas, deberá contar con las validaciones de cada etapa como se indica a continuación:

3.3.1. MÓDULO DE AUTORIZACIÓN

El módulo de autorización comprende todo el proceso llevado a cabo desde la creación de la solicitud de autorización de una rifa en la plataforma del operador tecnológico hasta la autorización final para la operación de las rifas correspondientes. Este módulo debe contener los siguientes sub-módulos, que se habilitarán uno a uno, previo al cumplimiento de lo requerido en el submódulo que lo antecede. A continuación, se indica la funcionalidad de cada uno:

3.3.1.1. SUBMÓDULO DE CREACIÓN DE UNA RIFA

La creación inicia cuando el gestor registra los siguientes datos:

1. Razón social y domicilio del responsable de la rifa.
2. Fotocopia de cédula de ciudadanía si se trata de persona natural; Certificado de Existencia y Representación Legal, expedido por la correspondiente Cámara de Comercio y fotocopia de la Cédula de Ciudadanía del representante legal si se trata de persona jurídica.
3. Nombre de la rifa.
4. Fecha de inicio de la venta de la rifa.
5. Fecha de finalización de la venta de la rifa.
6. Valor de venta al público de cada tiquete y/o boleta.
7. Número total de tiquetes y/o boletas que se emitirán.
8. Valor del total de la emisión y,
9. Plan de premios que se ofrecerá al público, el cual contendrá la relación detallada de los bienes muebles, inmuebles y/o premios objeto de la rifa, especificando su naturaleza, cantidad y valor comercial incluido el IVA.

   Esta información deberá ser suministrada de manera desagregada de tal manera que se identifiquen los valores que corresponden con IVA y sin IVA. (Validar cálculo en cada premio)

En este paso se realiza la validación automática de lo siguiente:

- ✓ Tasa de retorno del plan de premios de acuerdo con la siguiente regla:
- ✓ Plan de premios. Equivalente mínimo al 40% del valor total de la emisión antes de IVA o de acuerdo con la normativa vigente.

Una vez verificado el cumplimiento del plan de premios, se habilita el cargue de los documentos relacionados en el Decreto 1068 del 2015 modificado por el Decreto 1486 del 2024.
Las solicitudes de autorización para la gestión de rifas deberán presentarse con la anterioridad establecida en la normativa y legislación vigente. Lo anterior, debe garantizarse desde la plataforma al momento de la creación de una rifa.

3.3.1.2. SUBMÓDULO DE GESTIÓN DE DOCUMENTOS.

El submódulo de gestión de documentos estará habilitado exclusivamente para los gestores previamente registrados en la plataforma y que cuente con lo dispuesto en el submódulo de "Creación de una rifa".
Conforme a lo dispuesto en el Decreto 1068 del 2015 modificado por el Decreto 1486 del 2024, los documentos que el gestor deberá cargar en este submódulo son los siguientes:

1. Comprobante de la plena propiedad sin reserva de dominio, de los bienes muebles e inmuebles o premios objeto de la rifa, lo cual se hará conforme con lo dispuesto en las normas legales vigentes.
2. Avalúo comercial de los bienes inmuebles y facturas o documentos de adquisición de los bienes muebles y premios que se rifen.
3. Garantía de cumplimiento contratada con una compañía de seguros constituida legalmente en el país, expedida a favor de la entidad competente de emitir la autorización. El valor de la garantía será igual al valor total del plan de premios y su vigencia por un término no inferior a cuatro (4) meses contados a partir de la fecha de realización del sorteo. Esta garantía podrá sustituirse por una de carácter bancario en los términos y condiciones anteriormente mencionados.
4. Texto del tiquete y/o boleta electrónica, en el cual debe contener como mínimo los siguientes datos:

a. Códigos de barras y/o códigos QR (Quick Response) que serán utilizados para los tiquetes y/o boletas electrónicas que se expidan en la venta y comercialización de la rifa.
b. El número de la boleta;
c. El valor de venta al público de la misma;

d. El lugar, la fecha y hora del sorteo; cabe resaltar que para el registro de la fecha del sorteo, la plataforma debe bloquear de manera automática los 30 días siguientes a la fecha del proceso de solicitud de autorización de la rifa.
e. El término de la caducidad del premio;
f. El espacio que se utilizará para anotar el número y la fecha del acto administrativo que autorizará la realización de la rifa;
g. La descripción de los bienes objeto de la rifa, con expresión de la marca comercial y si es posible, el modelo de los bienes en especie que constituye cada uno de los premios;
h. El valor de los bienes en moneda legal colombiana;
i. El nombre, domicilio, identificación y firma de la persona responsable de la rifa;
j. El nombre de la rifa;
k. La circunstancia de ser o no pagadero el premio al portador.
l. El nombre de la Lotería tradicional o de billetes con la cual se realizará el sorteo, según sea el caso.

5. Texto del proyecto de publicidad con que se pretenda promover la venta de boletas de la rifa, la cual deberá cumplir con el manual de imagen corporativa de la autoridad que autoriza su operación.

6. Autorización de la lotería tradicional o de los billetes cuyos resultados serán utilizados para la realización del sorteo, cuando haya lugar.

Así las cosas, las autoridades competentes podrán acceder al SGR mediante el usuario y clave suministrada por el Operador tecnológico para proceder con la validación completa de la documentación, pudiendo aprobar o rechazar los documentos uno a uno o en su conjunto de acuerdo a su estado de cumplimiento.

En el evento en que un documento deba ser requerido, el submódulo contará con un campo de texto para describir las razones por las que se debe subsanar.

Cuando la totalidad de los documentos sean aprobados por parte de la autoridad competente, se habilita el submódulo 2.3. "liquidación", donde la plataforma tecnológica realizará el cálculo automático de los derechos de explotación, gastos de administración y demás pagos aplicables según la normativa vigente, con base en la información que el gestor suministró al momento del registro de la solicitud de autorización de la rifa.

Lo expuesto se encuentra sujeto a los cambios, actualizaciones, modificaciones y peticiones adicionales que sean de consideración de las Autoridades Competentes conforme a la normativa vigente.

3.3.1.3. SUBMÓDULO DE LIQUIDACIÓN

Habilitado este submódulo, la plataforma tecnológica calculará automáticamente lo siguiente:

- Liquidación de derechos de explotación: 14% sobre el valor total de la emisión o de acuerdo con la normativa vigente.
- Liquidación de gastos de administración: 1% sobre el valor total de los derechos de explotación o de acuerdo con la normativa vigente.
- Liquidación del impuesto de timbre: 1% sobre el valor total de los derechos de explotación cuando estos superen los 6.000 UVT o de acuerdo con la normativa vigente.
- Liquidación valor total a pagar por parte del gestor: corresponde a la sumatoria de todos y cada uno de los valores liquidados por este submódulo.
- Los demás aspectos requeridos por parte de las autoridades competentes en concordancia de la normativa vigente.

Todas las cifras calculadas en el presente submódulo se liquidan sobre valores sin incluir el IVA.

Lo expuesto se encuentra sujeto a los cambios, actualizaciones, modificaciones y peticiones adicionales que sean de consideración de las Autoridades Competentes conforme a la normativa vigente.

3.3.1.4. SUBMÓDULO DE PAGO

Este submódulo permitirá al gestor seleccionar el método de pago a utilizar de los dispuestos por la autoridad competente, de los cuales se excluyen las integraciones entre plataformas para pagos. Una vez realizado el pago, el gestor deberá cargar el respectivo soporte según haya lugar.

Lo expuesto anteriormente se encuentra sujeto a los cambios, actualizaciones, modificaciones y peticiones adicionales que sean de consideración de las Autoridades Competentes conforme a la normativa vigente.

3.3.1.5. SUBMÓDULO DE PROCESO DE NOTIFICACIÓN (AUTORIZACIÓN)

Una vez la autoridad competente haya validado el soporte del pago efectuado por el gestor, la plataforma tecnológica enviará un mensaje informativo vía correo electrónico y por los demás medios de comunicación que autorice el gestor y que disponga el operador tecnológico, en el

que se indique al Gestor que el acto administrativo de autorización de la rifa se encuentra en proceso de generación y notificación, lo cual será igualmente visible en el estado del trámite.

Una vez notificado y ejecutoriado el acto administrativo de autorización de la rifa por parte de la autoridad competente, ésta procederá a cargarlo en la plataforma del operador tecnológico junto con su constancia de ejecutoria, habilitando la comercialización de la rifa, lo cual efectuará automáticamente el sistema para la fecha de inicio de venta registrada por el gestor al momento de la creación de la solicitud de autorización de la rifa o la fecha de ejecutoria del acto administrativo de autorización que registre al momento de dicho cargue, lo último que ocurra, y hasta la fecha de finalización registrada igualmente por el gestor al momento de la solicitud. En todo caso, el inicio de la venta no será anterior a la fecha de cargue de los documentos mencionados.

Lo expuesto se encuentra sujeto a los cambios, actualizaciones, modificaciones y peticiones adicionales que sean de consideración de las Autoridades Competentes conforme a la normativa vigente.

3.3.1.6. SUBMÓDULO DE SOLICITUDES

Por medio de este submódulo, la plataforma deberá permitirle al gestor realizar las siguientes solicitudes según sea el caso:

- **Reprogramación de sorteos:** Esta solicitud podrá ser realizada cuando el sorteo deba ser aplazado o que no exista un ganador como resultado del primer sorteo.

- **Devolución de rentas pagadas:** Esta solicitud podrá ser realizada luego del cierre del plazo de comercialización de las rifas conforme a lo dispuesto en el submódulo **"3.3.2.2 CIERRE DE COMERCIALIZACIÓN Y PROCESO DE RELIQUIDACIÓN (DEVOLUCIÓN)".**

En este submódulo se deberán registrar todas las solicitudes que den lugar y que el gestor deba realizar para la gestión y comercialización de sus rifas.

3.3.2. MÓDULO DE COMERCIALIZACIÓN.

Este módulo comprende el proceso de venta de la rifa, donde el gestor, la autoridad competente y el CNJSA, según corresponda, podrán consultar en línea y en tiempo real el estado de la totalidad de la boletería autorizada, que deberá estar disponible desde el primer de comercialización. Este módulo deberá mantener actualizado en línea y tiempo real y desde el

inicio de la comercialización de la rifa, el estado de las boletas emitidas en cada rifa, que podrá ser:

- ✓ **AUTORIZADAS:** Corresponde al estado con el que antes del inicio del plazo de comercialización el SGR debe marcar la totalidad de las boletas emitidas, las cuales corresponden a las autorizadas mediante acto administrativo, conforme a lo registrado por el gestor en el trámite de solicitud de autorización de la rifa.
- ✓ **DISPONIBLE**: Es el estado de todas las boletas autorizadas a partir del inicio de la vigencia de comercialización que indica que podrá ser comprada por un jugador.
- ✓ **NO VENDIDA:** Este estado debe generarse de manera automática por el SGR sobre las boletas que a la finalización del plazo de comercialización se encuentren en estado "DISPONIBLE". Estas boletas no participan del sorteo.
- ✓ **VENDIDA:** Este estado debe generarse de manera automática por el SGR durante el plazo de comercialización sobre las boletas "DISPONIBLES" que son adquiridas por los jugadores y/o apostadores.
- ✓ **RESERVADA:** Este estado corresponde a las boletas que se encuentren en proceso de compra, la plataforma deberá bloquear temporalmente (10 minutos) los números seleccionados por el usuario hasta que se efectúe la compra o transcurra el tiempo definido, lo que ocurra primero. Si transcurrido los 10 minutos, no se registra el pago del boleto, automáticamente este regresará al estado "DISPONIBLE". En caso del cierre de la comercialización la boleta cambiará a estado "NO VENDIDA".
- ✓ **GANADORA:** Este estado es marcado automáticamente por el SGR sobre la boleta cuyo número coincide con el resultado del sorteo.

Una vez autorizada la rifa, el proceso de venta inicia con la habilitación de la comercialización de la rifa en los términos previstos en el submódulo **"3.3.1.5. SUBMÓDULO DE PROCESO DE NOTIFICACIÓN (AUTORIZACIÓN)"**.

Para la venta por internet, el apostador deberá registrarse como usuario dentro de la plataforma dispuesta para la venta.

3.3.2.1. REGISTRO DEL APOSTADOR EN EL CANAL DE VENTA POR INTERNET

El SGR debe contar con un sitio web que permita habilitar las ventas del juego de suerte y azar RIFAS de forma segura, que por medio de Dispositivos de Conexión Remota (DCR) a través de canales interactivos permitan al SGR como mínimo identificar la ubicación georreferenciada del jugador para controlar, según sea el caso, los límites de la territorialidad de la rifa, recibir toda la información correspondiente a las apuestas de un jugador y generar tiquetes electrónicos.

El proceso de registro e identificación del jugador se hará en el SGR, donde se dispondrá de un formulario de registro virtual para ser diligenciado por el jugador con el fin de obtener su cuenta de usuario y acceder a la zona transaccional del juego para realizar la compra de boletos por internet. Este registro será realizado por el jugar por una única vez.

El formulario de registro debe contener mínimo los siguientes datos:

- Tipo de identificación
- Número de identificación
- Primer nombre
- Segundo nombre (Opcional)
- Primer apellido
- Segundo apellido (Opcional)
- Género
- Fecha de nacimiento
- Lugar de nacimiento
- Fecha de expedición del documento de identificación
- Lugar de expedición del documento de identificación
- Fecha de vencimiento de la cédula de extranjería (Si aplica)
- Dirección de correo electrónico
- Teléfono móvil
- Ubicación del municipio (Cód. DANE)

De otra parte, la plataforma debe contar con la capacidad de garantizar mínimo los siguientes aspectos para la gestión de venta de boletas por internet:

- El operador tecnológico debe establecer un procedimiento para la actualización de la información del jugador, mínimo cada 12 meses.

- Solo debe permitir una sesión transaccional por usuario y en un solo DCR, no permitirá sesiones simultáneas del mismo usuario.

- Al momento de realizar la compra, el apostador deberá tener la opción de elegir el boleto (número o números) a comprar o elegir que el sistema le asigne uno aleatoriamente a través de un GNA.

- Implementar un mecanismo de verificación para validar la ubicación de la compra por parte del jugador (Latitud y Longitud).

- Implementar un mecanismo de verificación de autenticidad de la identidad del jugador al momento del registro en la plataforma del juego.

- Dar cumplimiento a las disposiciones de la Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones, o las normas que la modifiquen, complementen o reemplacen.

- Para el registro de los apostadores, el Operador Tecnológico debe garantizar que la captura, almacenamiento y tratamiento de datos personales cumpla con lo dispuesto por la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa que la modifique, complemente o reemplace.

- La transmisión de información gestionada a través del SGR, deberá estar cifrada con una clave no inferior a 2048 bits. El certificado de cifrado debe ser emitido por una autoridad certificadora (Certification Authority) reconocida por los navegadores más comunes.

- Cualquier incidente de seguridad o vulneración de datos personales deberá ser notificado a las autoridades competentes y a los usuarios afectados dentro de los plazos establecidos por la ley.

- El SGR que se utilice para el canal de venta por internet deberá identificar el lugar geográfico en donde se realizó la apuesta con el correspondiente código de municipio, según lo establecido por el Departamento Administrativo Nacional de Estadística –DANE-. Así mismo, para las rifas de carácter nacional se debe restringir la venta de boletas fuera del territorio colombiano. Para las rifas autorizadas por entidades territoriales se debe restringir la venta de boletas fuera del territorio para el que se emitió el acto administrativo de autorización.

- Establecer un mecanismo de confirmación de la apuesta previo al pago de la boleta.

- Disponer de los medios de pago para realizar la compra de las apuestas, como lo son:
    a. Transferencias desde cuentas bancarias.
    b. Tarjetas débito o crédito avaladas y emitidas por entidades autorizadas y vigiladas por la Superintendencia Financiera de Colombia.
    c. Cualquier otro medio de pago de los autorizados por la Superintendencia Financiera de Colombia.
    d. Pagos en efectivo.

Para efectos de garantía de confidencialidad, el intermediario utilizado debe cumplir la Norma de Seguridad de Datos (DSS) de la industria de Tarjetas de Pago (PCI) en su versión más reciente.

- La operación del canal de apuesta por internet se deberá realizar bajo los lineamientos definidos por el Operador tecnológico que garanticen la seguridad de las transacciones realizadas por el jugador registrado, debe tener la funcionalidad necesaria para generar la siguiente información a transmitir al SGR:

    a. Toda la información correspondiente a la apuesta.

    b. Consulta de sorteos y pago de premios.

    c. Generación del número aleatorio para definir la combinación de los "N" números de la jugada cuando se elige la opción de apuesta automática.

    d. La información de control.

    e. La ubicación geográfica donde se realiza la transacción.
- Capacidad de recibir compra de boletos hasta 1 día hábil anterior al sorteo y hasta la hora definida por el gestor. Posterior a esa hora, se deberán bloquear las ventas y anulaciones en todos los canales de comercialización. Además, el gestor deberá enviar por medio de correo electrónico al CNJSA el reporte de la boletería vendida, no vendida y anuladas a más tardar el día hábil anterior al sorteo. El día del sorteo no se pueden comercializar boletas. Cabe resaltar que dicha información también deberá reposar en la plataforma para ejecutar las respectivas acciones de vigilancia y control del proceso del actor con el rol correspondiente.

- El operador tecnológico deberá definir procedimientos para evitar que los menores de edad puedan realizar la apertura de cuentas de apostadores, para lo cual deben verificar la edad del jugador y establecer las restricciones necesarias para evitar el acceso a aquellos que no acrediten la mayoría de edad. El sistema no debe permitir el registro de personas que no cumplan la mayoría de edad, esto es, 18 años.

- Los usuarios registrados podrán realizar apuestas a través de su cuenta siempre y cuando esté “habilitada”. El operador tecnológico podrá establecer estados para la cuenta diferentes a “habilitada/activa/suspendida”, en cuyo caso podrá restringir el uso de la plataforma parcial o totalmente. El operador tecnológico podrá limitar el uso del canal de ventas por internet y establecer restricciones para usuarios que den mal uso de ellas.

Los proveedores del servicio de conectividad, ya sea el Operador tecnológico o un tercero, deben permitir la realización de pruebas de conexión entre el canal de apuestas por internet y el SGR, para lo cual deben disponer de todas las herramientas de hardware y software, los entornos y el personal necesario para la correcta realización de dichas pruebas.

El SGR no debe permitir el acceso a usuarios no registrados.

El SGR debe tener la capacidad para suspender en cualquier momento la realización de apuestas en internet en caso de detectarse su uso no autorizado.

3.3.2.2. CIERRE DE COMERCIALIZACIÓN Y PROCESO DE RELIQUIDACIÓN (DEVOLUCIÓN)".

El plazo de comercialización de la rifa será el que corresponda conforme a lo dispuesto en el "**3.3.1.5. SUBMÓDULO DE PROCESO DE NOTIFICACIÓN (AUTORIZACIÓN)**". El SGR finalizará de manera automática el plazo de comercialización de la rifa una vez se cumpla la fecha registrada por el gestor al momento de la solicitud. No obstante, la finalización del mencionado plazo podrá ser anterior a la fecha registrada por el gestor, cuando la totalidad de las boletas emitidas hayan sido vendidas y/o reportadas como no disponibles por encontrarse invalidadas, evento en el cual, el gestor podrá finalizar en el SGR de manera anticipada y manual la comercialización de la rifa.

Finalizada la comercialización y teniendo en cuenta el total de las boletas efectivamente vendidas, el SGR de manera automática realizará la reliquidación de las obligaciones económicas inicialmente pagadas por el gestor, sin limitar a: i) Derechos de explotación, ii) Gastos de administración, e iii) Impuesto de timbre (si aplica). Lo anterior, con el fin de determinar si procede la devolución de valor alguno al gestor frente a lo inicialmente liquidado y pagado. El SGR calculará automáticamente el monto a devolver al gestor en caso de que aplique.

Para ejecutar la devolución, el SGR debe permitir el cargue de documentos exigidos por cada autoridad competente a través del "**3.3.1.6. SUBMÓDULO DE SOLICITUDES**".

Esta información es generada en el SGR de acuerdo a lo descrito en el artículo 2.7.3.7 parágrafo 1° del Decreto 1068 de 2015 modificado por el artículo 7 del Decreto 1486 de 2024.

3.3.3. SORTEOS

3.3.3.1. PARAMETRIZACIÓN DE SORTEOS EN EL SGR

- **SORTEO POR GENERADOR DE NUMEROS ALEATORIOS – GNA –**

Una vez se surta el proceso de autorización, el SGR deberá generar un enlace único hacia una página web pública que deberá contar con un botón que redirija a los usuarios al registro o al inicio de sesión para la compra de boletas. Este enlace deberá estar dentro del dominio principal que registre el Operador Tecnológico y será usada por cada Gestor en las transmisiones de sorteos vía streaming, es decir, este enlace contendrá la visual del sorteo además de las respectivas métricas e información de interés que considere el gestor sean pertinentes compartir a los usuarios apostadores.

El sorteo se deberá realizar en línea y en tiempo real a través de la página web pública y el SGR deberá generar de manera automática el número ganador en la fecha y hora autorizada mediante el acto administrativo. El Gestor trasmitirá el sorteo vía streaming en las plataformas de su elección.

La página web para los sorteos estará habilitada hasta el cierre de la rifa y los resultados de los sorteos reposarán en el SGR.

- **RESULTADOS CONTRA LOTERÍA**

Cuando la rifa se lleve a cabo contra resultados del premio mayor de alguna lotería tradicional, el gestor deberá registrar de manera manual e inmediatamente realizado el sorteo, el resultado ganador en el SGR.

Los roles de, Operador Tecnológico, Gestor y Usuario deberán contar con un submódulo de "Sorteos" para lo cual, la plataforma deberá disponer de las siguientes consideraciones:

- **Operador Tecnológico:** Para las rifas realizadas contra los resultados del premio mayor de las loterías tradicionales, el operador tecnológico deberá disponer de los siguientes campos de registro por parte del gestor:
    - Campo 1: Número ganador una vez se genere el sorteo.
    - Campo 2: Link o enlace que redirige a los resultados de la lotería para su validación.

- Cuando la rifa se lleve a cabo contra resultados de sorteos realizados mediante un GNA, la plataforma deberá generar y registrar de manera automática los campos relacionados anteriormente.

  Para ambos casos, si el número ganador corresponde a una boleta no vendida, la plataforma deberá marcar el sorteo automáticamente como "próximo a reprogramar".

- **Gestor**: Para las rifas realizadas contra los resultados del premio mayor de las loterías tradicionales, el gestor deberá diligenciar los dos campos que ha dispuesto el Operador tecnológico en el SGR (Campo 1 y Campo 2).

  Cuando la rifa se lleve a cabo contra resultados de sorteos realizados mediante un GNA, el Gestor deberá utilizar el link que le generó el SGR al momento de surtir el proceso de autorización de la rifa de acuerdo a lo indicado en el inciso primero del numeral "**3.3.3.1. PARAMETRIZACIÓN DE SORTEOS EN EL SGR. "**

  Si el número ganador corresponde a una boleta no vendida, el gestor deberá iniciar con la solicitud de reprogramación de un nuevo sorteo.

- **Usuario:** Para las rifas realizadas contra los resultados del premio mayor de las loterías tradicionales, la plataforma deberá disponer de los siguientes campos:
  - Campo 1: El número ganador registrado una vez se ha ejecutado el sorteo.
  - Campo 2: El link que redirige a la página web de la lotería para constatar los resultados.

  El usuario podrá conocer el histórico de resultados en su Dashboard, además, la plataforma deberá disponer de los botones (Facebook, X, YouTube, Kick, etc.) que considere el Gestor sean necesarios para redirigir a los usuarios a la o las plataformas de transmisión streaming del gestor.

3.3.4. VERIFICACIÓN DE GANADOR

Cuando la rifa se realice contra los resultados de sorteos por GNA, el SGR automáticamente deberá validar e identificar si el número ganador se encuentra dentro de las boletas "VENDIDAS"

Cuando la rifa se realice contra los resultados del premio mayor de una lotería tradicional que opere legalmente en Colombia, el gestor deberá ingresar manualmente dicho resultado en el SGR con el fin que este automáticamente valide e identifique si el número ganador se encuentra dentro de las boletas "VENDIDAS".

En cualquiera de los dos tipos de sorteos, en caso de identificarse ganador, el SGR deberá activar automáticamente el inicio del plazo que tiene el ganador para reclamar su premio (1 año contado a partir de la fecha de realización del sorteo), e identificar el plan de premios como "pendiente por reclamar". Si la boleta ganadora corresponde a una venta realizada por internet (Boleta nominal), la plataforma deberá informar por medio de un correo electrónico tanto al jugador como al gestor que hubo un ganador, remitiendo al ganador un código único de verificación para la reclamación del premio.

Cuando la venta sea realizada por medio de una terminal de venta fija y/o sea una apuesta anónima (Boleta al portador), solamente será notificado el gestor por medio de correo electrónico que indique que hubo un ganador.

Seguidamente, si el ganador reclama el plan de premios, la plataforma deberá permitirle al gestor realizar el cargue de los documentos que el ganador suministre como soportes para la validación de su identidad.

Si transcurrido el plazo establecido en la normativa vigente para reclamar el (los) premios, y estos no han sido reclamados, el SGR deberá identificar el plan de premios como "prescrito" y el gestor deberá proceder en los términos y plazos de ley a transferir a la salud los recursos según corresponda.

Si no se identifica GANADOR el SGR deberá permitir al gestor solicitar ante la autoridad competente una nueva fecha para la realización del sorteo, hasta que el premio o los premios queden en poder del público, para lo cual el gestor deberá cargar en el SGR los soportes previstos en el inciso 2 y 3 del artículo 2.7.3.8 del Decreto 1068 de 2015 modificado por el Decreto 1486 de 2024. En ningún caso después de cerrada la rifa, se podrá habilitar nuevamente la comercialización de la misma.

Cuando la boleta sea expedida por una terminal de venta física, se considera que es un documento al portador, por tal razón el gestor deberá verificar previo a la entrega del premio la veracidad de la boleta o tiquete, teniendo en cuenta la siguiente información:

- ✓ **FECHA DEL SORTEO:** Deberá validarse si corresponde a la fecha predeterminada por el gestor en el momento de la solicitud o en las re programaciones autorizadas por la autoridad competente.
- ✓ **RESULTADO DEL SORTEO**: Deberá validarse si el número registrado en el tiquete corresponde a los resultados del sorteo de la lotería autorizada o resultado mediante GNA.

- ✓ **CÓDIGO HASH DEL BOLETO:** Se deberá constatar el código hash del tiquete ganador en donde se evidencie que este corresponde a la boleta vendida.

Cuando la venta se realice a través de internet y/u otro mecanismo tecnológico, el SGR deberá validar de manera automática la identidad del ganador basado en los datos de registro del mismo. El SGR deberá enviar al ganador un código único de verificación para la reclamación del premio, el cual deberá suministrar al gestor en el momento que se realice el proceso de reclamación del premio. Este código deberá estar activo hasta un año más, contado a partir de la realización del sorteo.

3.3.4.1. VERIFICACIÓN DE LA.ENTREGA DEL PREMIO

De acuerdo con lo dispuesto en el *"Artículo 2.7.3.11. Verificación de la entrega del premio"* del Decreto 1068 de 2015, modificado por el artículo 10 del Decreto 1486 de 2024.

> *(...) "El gestor deberá presentar ante la autoridad competente a través del operador, máximo dentro de los cinco (5) días hábiles siguientes a la entrega de los premios, la declaración jurada ante notario por la persona o personas favorecidas con el premio o premios de la rifa realizada en la cual conste que recibieron los mismos a entera satisfacción. La inobservancia de este requisito impide al gestor tramitar y obtener autorización para la realización de futuras rifas." (...)*
>
> *PARÁGRAFO. En el caso de que las rifas se operen por los concesionarios del juego de apuestas permanentes o por las entidades que operen la Lotería tradicional o de billetes, la declaración jurada de la entrega del premio ante notario podrá ser reemplazada por acta suscrita por el ganador y certificación del revisor fiscal o contador y representante legal de la respectiva empresa*

A partir del momento en que el premio sea entregado, el SGR deberá activar automáticamente el tiempo máximo de cinco (5) días hábiles para que el gestor presente ante la autoridad competente y a través de la plataforma tecnológica, los soportes de la entrega del premio, conforme a lo previsto en el artículo 2.7.3.11 del Decreto 1068 de 2015, modificado por el Decreto 1486 de 2024 o la norma que lo modifique o sustituya.

Nota: El SGR deberá permitir que los documentos relacionados sean cargados exclusivamente en formato PDF.

4. DESARROLLO DEL SOFTWARE GESTIÓN DE RIFAS (SGR).

La primera fase de análisis implica no sólo la recopilación de requisitos técnicos, sino una validación profunda de la operatividad del sistema en condiciones reales. Es imprescindible que los procesos manuales susceptibles de automatización sean identificados y ajustados para su respectiva integración en la plataforma por parte del Operador Tecnológico. Del mismo modo, se deben considerar las necesidades normativas, asegurando que todas las funcionalidades cumplan con los estándares regulatorios y de seguridad exigidos.

El diseño del sistema debe centrarse en una arquitectura flexible, capaz de escalar y adaptarse a los cambios futuros del sector de los juegos de suerte y azar en Colombia. El Operador Tecnológico debe garantizar que los módulos funcionen de manera independiente, pero que mantengan una integración fluida entre sí. Desde la capa de presentación, hasta la capa de seguridad, que deberá contener protocolos de autenticación robustos y encriptación avanzada, aportando un diseño con enfoque centrado en la eficiencia y la confiabilidad. Durante esta fase de diseño, la experiencia del usuario juega un papel fundamental, ya que la interfaz debe ser intuitiva y accesible para todos los actores involucrados.

Antes de la implementación, el sistema debe pasar por una fase de preproducción en la que se validarán los procesos con datos reales. Durante esta etapa, se simularán transacciones masivas para evaluar la capacidad del sistema, se verificará la interoperabilidad con plataformas externas y se realizarán auditorías de seguridad para certificar su cumplimiento con las regulaciones vigentes. Es imprescindible que las Autoridades Competentes sean capacitadas adecuadamente, garantizando que cualquier incidente pueda ser gestionado de manera rápida y eficiente.

La fase de pruebas determinará la estabilidad del SCJ antes de su despliegue definitivo. Se realizarán pruebas unitarias para validar cada módulo de manera independiente, pruebas de integración para verificar la comunicación entre ellos y pruebas de carga para evaluar su rendimiento bajo condiciones de alta demanda. Adicionalmente, se ejecutarán pruebas de seguridad para identificar vulnerabilidades y mitigar posibles riesgos antes de la puesta en producción. Una vez superadas todas estas evaluaciones, se procederá a la implementación en la infraestructura de producción, asegurando la disponibilidad del sistema y estableciendo mecanismos de monitoreo en tiempo real para detectar y solucionar cualquier anomalía.

Se debe contemplar la actualización periódica de funcionalidades y la optimización de procesos con base en el análisis continuo de datos. La supervisión constante por parte del Operador Tecnológico y la interacción con las Autoridades Competentes permitirán una evolución progresiva del SGR, garantizando que se mantenga alineado con los requisitos normativos y las

necesidades del mercado. La solidez del SGR dependerá no solo de su desarrollo técnico, sino de la rigurosidad con la que se aborden cada uno de estos módulos y submódulos, asegurando su correcto funcionamiento y operatividad desde el primer día de implementación.

El desarrollo del SGR, debe garantizar su estabilidad y seguridad en todas las fases previas a la implementación. Para ello, el Operador Tecnológico debe llevar a cabo una ingeniería de detalle en conjunto con las Autoridades Competentes, asegurando el cumplimiento de los aspectos técnicos, misionales y funcionales en las etapas de pruebas, preproducción y producción.

5. HARDWARE Y SOFTWARE DISPUESTO PARA LAS AUTORIDADES COMPETENTES

El hardware y/o software requerido para el control y auditoría del juego de suerte y azar RIFAS conforme a lo definido en el presente numeral, estará a cargo de las autoridades competente y el CNJSA y será dispuesto por el operador tecnológico.

La metodología de control y auditoría del juego de suerte y azar RIFAS será fundamentada en un sistema especializado de herramientas (Hardware y Software) y procedimientos para garantizar la transparencia, seguridad y cumplimiento normativo. De manera adicional, el operador deberá asumir los costos por soporte y mantenimiento de todos los componentes (hardware y software) durante todo el periodo de la concesión y dos (2) años adicionales.

5.1. REQUISITOS GENERALES DE LA TERMINAL DE VENTA - TDV

La operación de las terminales de venta se realizará bajo los lineamientos definidos por el Operador tecnológico que garanticen la seguridad de las transacciones. Estos dispositivos deben tener la funcionalidad necesaria para generar mínimo la siguiente información a transmitir al SGR:

- Toda la información correspondiente a la apuesta.
- La información de control o eventos significativos que se generen desde la TDV.
- La ubicación geográfica donde se realiza la transacción (Código DANE del Departamento y municipio, así como la latitud y longitud donde se hizo la compra).

Los proveedores del servicio de conectividad ya sea del Operador tecnológico o un tercero, deben permitir la realización de pruebas de conexión entre los TDV y el SGR, para lo cual deben disponer de todas las herramientas de hardware y software, los entornos y el personal necesario para la correcta realización de dichas pruebas.

El software de administración de las TDV no debe permitir el acceso a usuarios no registrados en el SGR.

El SGR debe tener la capacidad para suspender la realización de ventas en un TDV en caso de detectarse el uso no autorizado de la misma, sin afectar otras terminales.

Las TDV ubicadas en los puntos de venta deben cumplir mínimo con las siguientes condiciones:

- Estar en sitios seguros de acceso controlado por parte del operador.
- La TDV debe tener su propia y única ID en el SCJ.
- El acceso a la operación del terminal debe estar restringido por contraseñas de seguridad y/o cualquier otro mecanismo de protección de acceso no deseado.
- Los cables que suministran la energía y los cables de datos que entran y salen de la terminal no deben ser accesibles al público en general y no podrán ser fácilmente removidos.
- Los puertos de comunicaciones de las terminales deben estar etiquetados e identificados adecuadamente de acuerdo a su función y deben estar dentro de un área segura para impedir acceso sin autorización al mismo o a sus cables de conexión.
- La interfaz de comunicaciones para la conexión al SGR debe estar localizada en un sitio seguro, al cual solamente se le permita el acceso a personal autorizado asignado por el Operador.

Las TDV móviles utilizados deben cumplir mínimo con las siguientes condiciones:

- Deben estar asociadas a un punto de venta con el código DANE de municipio a cada transacción. Adicionalmente, todas las ventas realizadas desde dicha terminal deben reportar tanto la latitud como la longitud donde se realizó la venta.
- El acceso a la operación del terminal, tanto para el software de administración de las TDV como de configuración técnica y demás perfiles que tengan acceso a las TDV, debe estar restringido por contraseñas de seguridad y/o cualquier otro mecanismo de protección de acceso no deseado. Además, este acceso debe quedar registrado en los Logs de las TDV para ser enviado al SCJ.
- La TDV móvil debe tener su propia y única ID en el SGR.

- La información debe ser transmitida (enviar/recibir), cifrada y aplicar algoritmos seguros de validación.

- Contar con seguridades de registro y transacciones de las TDV con el SGR. El proponente debe presentar las características del modelo de seguridad para la evaluación respectiva al laboratorio encargado de la certificación del SCJ.

5.2. REQUISITOS DE IDENTIFICACIÓN DE LA TERMINAL DE VENTA - TDV

Las TDV deben tener una identificación lógica única (ID) que permita reconocerla dentro del SGR. Esta identificación debe permitir determinar: si es un TDV fijo o móvil, el código del punto de venta asociado dentro del SGR para la TDV fijo o móvil y el código DANE del municipio donde opera.

5.2.1. IMPRESORA DE BOLETAS

Las TDV deben permitir imprimir la boleta objeto del sorteo del juego de suerte y azar RIFAS con la información indicada en el numeral 4 del artículo 2.7.3.6 del Decreto 1068 de 2015 modificado por el Decreto 1486 del 2024. La información de cada uno de los tiquetes o boletas deberá conservarse en el SGR por el mismo tiempo de la concesión del contrato y (2) dos años más.

5.2.2. DISPOSITIVOS DE CONEXIÓN REMOTA - DCR

La plataforma debe tener los mecanismos que permitan identificar la dirección IP del dispositivo y en la medida que técnicamente sea posible, identificar y registrar los diferentes tipos de dispositivos utilizados por los jugadores a través de canales interactivos adicionando los datos de la versión y sistema operativo. Las funcionalidades de los DCR estarán condicionados a los siguientes aspectos:

- El dispositivo únicamente se encargará de la interacción del jugador con la presentación web.

- Todas las transacciones realizadas a través del dispositivo serán registradas en la base de datos del SGR y asociadas al jugador que fue objeto de autenticación previa.

- Los registros permitirán identificar las transacciones realizadas desde cada dispositivo.

6. VENTA DE BOLETAS

Las boletas se podrán vender de manera física mediante una terminal de venta electrónica o a través de internet.

6.1. GENERACIÓN DEL BOLETAS ELECTRÓNICAS

El operador del juego de suerte y azar RIFAS debe disponer mecanismos para que el apostador pueda seleccionar distintos medios de pago electrónicos para la compra de la o las boletas.

Para el registro de la apuesta se debe generar un tiquete electrónico que servirá como comprobante de la transacción, este debe ser enviado a la cuenta de correo electrónico registrada y debe contener por lo menos la siguiente información:

INFORMACIÓN DE LA VENTA (Apuestas)	
Dato	Lista de Valores
Fecha Venta Tiquete	dd/mm/aaaa
Hora Venta Tiquete	hh:mm:ss
Código hash de seguridad de la venta	Código hash criptográfico que garantiza la integridad y autenticidad de los boletos.
Identificación Única Terminal de Venta	Identificación del terminal de venta en el Sistema Central de Juegos (Aplica para TDV) donde se realizó la venta
Número de la boleta	El número consecutivo de la boleta correspondiente
Valor de venta al público	El valor de venta al público.
Lugar, fecha y hora sorteo	El lugar, fecha y hora del sorteo.
Tipo de sorteo	Generador de números aleatorios (GNA) o por resultados del premio mayor de alguna lotería tradicional.
Nombre de la lotería (Si aplica)	Nombre de la lotería con la que se obtendrá el resultado ganador de la rifa.
Caducidad del premio	El término de la caducidad del premio
Número y fecha de acto administrativo	El espacio que se utilizará para anotar el número y la fecha del acto administrativo que autorizará la realización de la rifa.
Valor de bienes	El valor de los bienes en moneda legal colombiana

Responsable de la rifa (Gestor)	El nombre, domicilio, identificación y firma de la persona responsable de la rifa.
Nombre de la rifa	El nombre de la rifa
Premio al portador	La circunstancia de ser o no pagadero el premio al portador

INFORMACIÓN DE LA VENTA (Apuestas)	
Dato	Lista de Valores
Apuesta Individual	Valor o cifra elegida por el comprador para participar en un sorteo de rifa.
Valor apuesta individual	Valor apuesta individual
Ubicación donde se realizó la venta	Cód. Municipio DANE donde se realizó la venta: • Para las TDV el municipio de la ubicación de esta. • Para DCR-internet el municipio donde se encuentra localizada la IP del DCR.
Medio de pago con el que se realizó la venta	EF: Pagos en efectivo a través de puntos físicos establecidos por el Operador Para Internet: BC: Cuentas bancarias en entidades autorizadas CR: Tarjeta de crédito. IN: Instrumento de pago ofrecido por entidad vigilada por la Superintendencia Financiera de Colombia GI: Transferencia de giro PR: Tarjeta prepago recargable OT: Otro medio de pago ofrecido por el Operador.
Estado de la Boleta	Lista de Estado de la Boleta: 1. A: Autorizada 2. D: Disponible 3. R: Reservada (10 min) 4. V: Vendida 5. N: No vendida

	6. G: Ganadora

7. TECNOLOGÍA BLOCKCHAIN PARA LA EMISIÓN DE BOLETOS.

Para la emisión de los boletos en los diferentes canales se requiere de usar la tecnología Blockchain para el blindaje de la integridad de los mismos. Como estándar mundialmente probado para sellado y blindaje de tiquetes podemos mencionar a OpenTimestamps.

OpenTimestamps es una herramienta de código abierto que permite crear marcas de tiempo verificables para archivos y datos, utilizando la blockchain de Bitcoin. Proporciona pruebas de existencia e integridad, asegurando que un archivo exista en un momento específico y no ha sido alterado desde entonces. Esto se logra generando un hash criptográfico del archivo, que se incluye en un árbol de Merkle y se ancla en la blockchain de Bitcoin, garantizando una prueba inmutable sin necesidad de revelar el contenido del archivo.

> *"Un Árbol de Merkle es una estructura de datos compuesta por hashes de diferentes bloques de datos, y que sirve como resumen de todas las transacciones de un bloque. También se conoce como "Hash Tree". Esta estructura permite verificar de forma eficiente, y segura, el contenido de una gran cantidad de datos. Además, ayuda a verificar la consistencia y el contenido de los datos.*
>
> *En un Árbol de Merkle cada nodo de hoja está etiquetado con el hash de un bloque de datos y el nodo que no es hoja está etiquetado con el hash criptográfico de las etiquetas de sus nodos secundarios."*

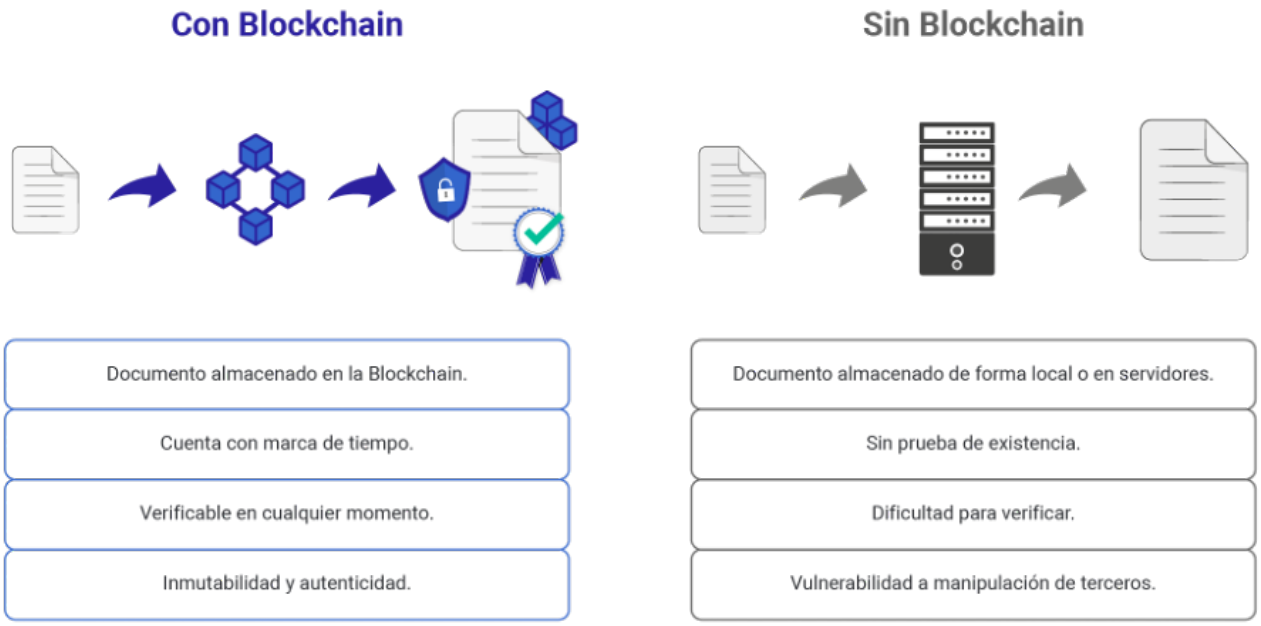


Ilustración 2. Comparativo de procesos para RIFAS con BLOCKCHAIN.

La implementación de esta tecnología ofrece múltiples beneficios y ventajas significativas, entre las cuales se pueden detallar las siguientes:

- Registro Inmutable*:* Blockchain proporciona un registro inmutable de todas las transacciones, lo que significa que una vez que un boleto se registra, no puede ser alterado.
- Verificación*:* Todas las transacciones son fácilmente verificables, permitiendo a las partes interesadas revisar el historial de cada tiquete de venta en cualquier momento.
- Criptografía*:* Blockchain utiliza técnicas criptográficas avanzadas para asegurar los datos, protegiéndolos contra fraudes y accesos no autorizados.
- Descentralización*:* Al no depender de un único punto de control, la descentralización reduce el riesgo de ataques cibernéticos centralizados.
- Reducción de intermediarios*:* Elimina la necesidad de intermediarios, lo que puede reducir costos y tiempos de transacción.
- Integridad de Datos*:* Los usuarios pueden confiar en que los datos almacenados en la blockchain son precisos y no han sido manipulados.
- Reputación*:* Las empresas que utilizan blockchain pueden mejorar su reputación al demostrar su compromiso con la transparencia y la seguridad.

7.1. ESQUEMA DE OPERATIVIDAD Y PROCESO TÉCNICO EN LA EMISIÓN DE BOLETOS.

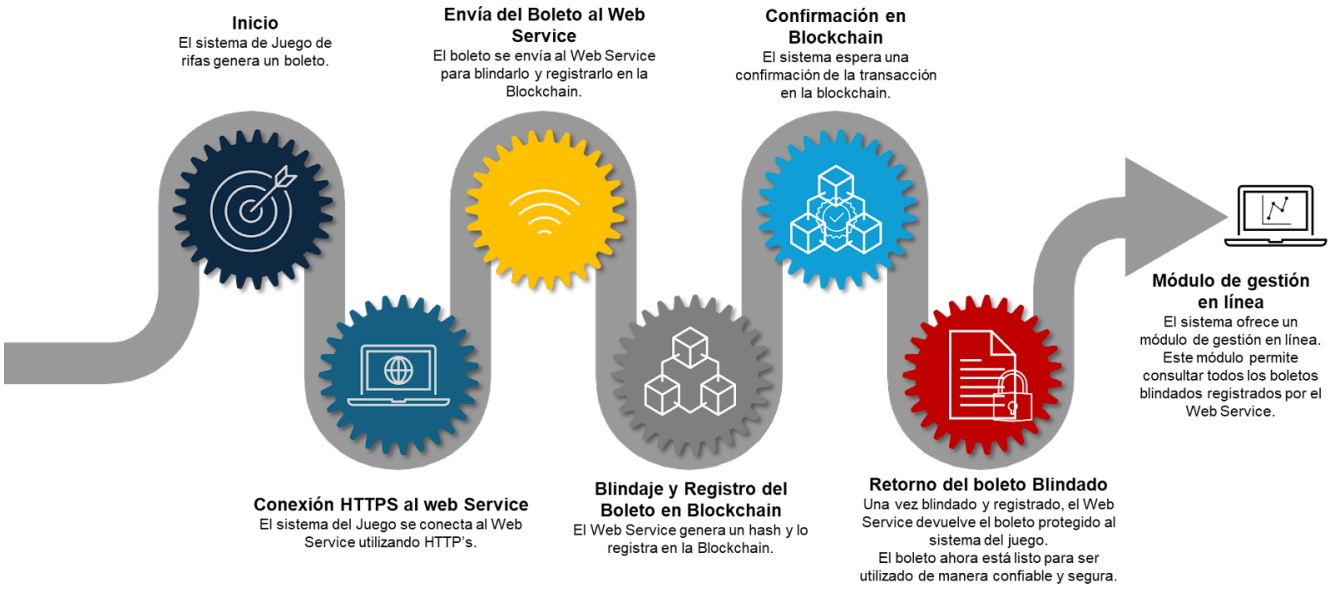


Ilustración 3. Proceso Técnico de operatividad RIFAS- BLOCKCHAIN

7.1.1. Inicio

En esta etapa, el sistema del juego de suerte y azar RIFAS produce un boleto de juego, que contiene toda la información necesaria para la participación en el juego y su respectiva validación. Este boleto es esencialmente un registro digital que será procesado y asegurado en blockchain.

7.1.2. Conexión HTTPS al Web Service

El sistema establece una conexión segura con un servicio web (Web Service) utilizando el protocolo HTTPS. Este protocolo asegura que los datos transmitidos entre el sistema del juego y el Web Service estén encriptados, protegiendo la integridad y confidencialidad del tiquete durante su transferencia.

7.1.3. Envío del boleto al Web Service

Una vez establecida la conexión segura, el sistema envía el boleto al Web Service. El propósito de esta acción es que el boleto sea procesado, protegido (blindado) y luego registrado en la blockchain para respaldar su integridad y autenticidad.

7.1.4. Blindaje y Registro del Boleto en Blockchain

El servicio de blindaje y registro del boleto en BlockChain, se debe hacer mediante un Web Service en la Nube. Este web Service debe tomar el boleto y le generará un código hash a través del algoritmo de seguridad criptografía SHA256. Este proceso es crítico para poder asegurar que el boleto no sea alterado o falsificado después de emitido.

Después de aplicar el algoritmo SHA256, el Web Service deberá enviar el hash que ha sido creado a la blockchain, para su posterior confirmación. La blockchain actúa como un registro inmutable y descentralizado, asegurando que la información del boleto esté permanentemente almacenada y pueda ser verificada en cualquier momento.

7.1.5. Confirmación en Blockchain

Cada transacción registrada requerirá un tiempo corto de confirmación. Sin embargo, es importante destacar que este intervalo de tiempo no afecta el flujo operativo ni causar demoras en el proceso general o en la verificación del boleto. Durante este período de confirmación, el boleto seguirá siendo completamente funcional y verificable, asegurando que el proceso continúe sin interrupciones o retrasos, garantizando la integridad y seguridad del boleto en todo momento.

7.1.6. Retorno del Boleto Blindado

Una vez completamente protegido y blindado, el Web Service devuelve el boleto al SGR. El boleto debe incluir un código QR que permita su verificación. Este código servirá como un medio eficiente y seguro para autenticar la validez del boleto, sea virtual o físico, garantizando así que los datos asociados puedan ser fácilmente confirmados mediante un escaneo rápido con dispositivos compatibles.

El código QR debe mostrar toda la información correspondiente al boleto generado tal cual como se describe en el punto **"6.1. GENERACIÓN DEL BOLETAS ELECTRÓNICAS"** y a su vez debe mostrar la información registrada en blockchain tales como, código hash del tiquete, número del bloque, enlace o URL del dato en blockchain, fecha y hora de la transacción y la confirmación de la transacción. Esto asegura la validez del boleto y que a su vez fue insertado y embebido en una blockchain que respalda la total confianza, seguridad y transparencia.

7.1.7. Módulo de Gestión en Línea

Se proporcionará un módulo de gestión en línea que permita a los operadores o usuarios autorizados acceder a la información de los boletos blindados.

A través de este módulo, es posible consultar, verificar, y gestionar todos los boletos que han sido blindados y registrados en la blockchain, asegurando la transparencia y accesibilidad de la información.

7.2. VERIFICACIÓN DE BOLETOS CON BLOCKCHAIN

Cualquier persona puede verificar la autenticidad del boleto de manera sencilla, contando con un sistema en línea con cualquiera de las tres formas de verificación:

1. Digitando el código único del boleto: El usuario deberá ingresar el código alfanumérico exclusivo asociado a su boleto. Este código actúa como identificador único que permite al sistema verificar y autenticar el boleto de manera precisa, garantizando que corresponde a una compra legítima y registrada en la blockchain.

2. Escaneo del código QR: El usuario podrá escanear el código QR de los boletos utilizando un dispositivo compatible, como un Smartphone o un lector de códigos QR. Este código contiene toda la información necesaria para autenticar el boleto de manera rápida y eficiente, independientemente de si el boleto es físico o digital.

3. Cargando o Arrastrando el boleto en formato PDF: El usuario podrá cargar el documento en formato PDF del boleto simplemente arrastrándolo y soltándolo en el área designada del sistema. Este proceso permitirá al sistema extraer y verificar

la información contenida en el PDF, asegurando que el boleto esté válido, correctamente registrado y autenticado.

Cada verificación exitosa confirmará la autenticidad del boleto, validando tanto la información del comprador como la del vendedor, además de toda la información registrada en la cadena de bloques para una total transparencia. Toda verificación debe mostrar la información correspondiente al tiquete generado tal cual como se describe en el apartado **"6.1. GENERACIÓN DEL BOLETAS ELECTRÓNICAS"** y a su vez debe mostrar la información registrada en blockchain tales como, código hash del boleto, número del bloque, enlace o URL del dato en blockchain, fecha y hora de la transacción y la confirmación de la transacción.

La transparencia proporcionada por blockchain también facilita la resolución de disputas, ya que todas las transacciones están registradas de forma clara y accesible para todas las partes involucradas, siendo este un paso crucial para garantizar un mercado más seguro, transparente, confiable, que protege a los apostadores y mitiga la ilegalidad.

8. REQUISITOS GENERALES DE FUNCIONALIDAD PARA EL GNA

El Generador de Números Aleatorios (GNA) es un sistema basado en hardware y/o software que genera valores numéricos aleatorios, utilizados para garantizar la transparencia y equidad en los

sorteos de los juegos de suerte y azar. Los requisitos de funcionalidad para el GNA son los siguientes:

- **Generación de resultados**: a) Generar de manera aleatoria la combinación de números seleccionada por el apostador en el caso de apuestas automáticas. b) Seleccionar de manera directa bajo criterio del apostador la combinación para su sorteo dentro de la cantidad de número posibles disponibles. Estos números serán utilizados para determinar el resultado del sorteo.
- **Características técnicas**: El GNA debe garantizar que los números generados sean:
    - Estadísticamente independientes: Cada número generado debe ser ajeno a los números anteriores o posteriores, asegurando la ausencia de patrones predecibles.
    - Impredecibles: Debe evitarse cualquier posibilidad de manipulación o predicción de los números generados.
    - Validados estadísticamente: Los resultados del GNA deben pasar pruebas estadísticas reconocidas (e.g., Chi-cuadrado, Kolmogorov-Smirnov, Entropía) para certificar su aleatoriedad.
- **Compatibilidad y disponibilidad**:
    - El GNA debe integrarse sin interrupciones con el software central encargado de la gestión del juego.
    - Debe estar disponible de manera continua para garantizar la emisión de tiquetes y la ejecución de sorteos en tiempo real.

8.1. TECNOLOGÍA BLOCKCHAIN PARA GNA

El Generador de Números Aleatorios - GNA, será implementado mediante contrato inteligente usando **Chainlink VRF (Verifiable Random Function)** en Blockchain. Así las cosas, el contrato inteligente que contenga el GNA y con el fin de garantizar la seguridad, confiabilidad y cumplimiento normativo del uso de los mismos. Se establece la obligatoriedad de auditorías de seguridad realizadas por firmas especializadas en el sector. Esta auditoría, deberá ser realizada exclusivamente por empresas de seguridad reconocidas en el ámbito de la tecnología blockchain y que cuenten con experiencia comprobable en la evaluación de código. El uso de cualquier contrato inteligente sin la certificación de al menos una empresa auditora, será considerado inválido y no podrá ser desplegado para la generación de números aleatorios.

Para la validación de un contrato inteligente, la empresa desarrolladora deberá presentar el informe de auditoría emitido por una de las firmas autorizadas, el cual debe incluir como mínimo:

- Revisión exhaustiva del código fuente.
- Identificación de vulnerabilidades críticas, altas, medias y bajas.
- Recomendaciones y correcciones de seguridad implementadas.
- Certificación de cumplimiento con los estándares de seguridad de la industria blockchain.

En caso de que el informe de auditoría indique la presencia de vulnerabilidades críticas o de alto impacto, el contrato no podrá ser implementado hasta que dichas vulnerabilidades sean mitigadas y verificadas.

El Operador tecnológico debe entregar toda la información relacionada con dicho Contrato Inteligente, incluyendo sin limitar: documentación, manuales, diagramas, información accesos lógicos y físicos, esquemas de bases de datos, arquitectura de hardware, software, servicios, y demás necesario para la realización de las pruebas requeridas. Así mismo, el costo asociado al proceso de auditoría será asumido por el operador y se deberá garantizar las pruebas y ensayos correspondientes.

Será responsabilidad del operador tecnológico la consecución de los GNA necesarios para la operación del juego, y de garantizar que las TDV que lo utilicen de forma intrínseca sean avaladas por el laboratorio certificador o por quien haga sus veces. Será responsabilidad del Operador tecnológico garantizar que dichos equipos se encuentren disponibles para la emisión del boleto y la realización de los sorteos.

La implementación de GNA en el juego de suerte y azar RIFAS mediante contratos inteligentes tiene el potencial de revolucionar la forma en que se manejan los sorteos. Utilizando blockchain, no solo se garantiza la aleatoriedad del proceso, sino que también se ofrece un nivel de transparencia superior: los participantes pueden verificar en tiempo real el proceso y los resultados, eliminando cualquier sospecha de manipulación o fraude.

Para la generación de números aleatorios en blockchain, se debe implementar el uso de **oráculos**, estos, permiten la obtención de números aleatorios de fuentes externas a los nodos de la cadena de manera verificable y segura.

En el contexto de Chainlink VRF (Verifiable Random Function), un "Oráculo" es un nodo descentralizado que proporciona datos externos y confiables a contratos inteligentes en la blockchain. En el caso específico de Chainlink VRF, el oráculo cumple una función importante al generar y verificar valores aleatorios de manera transparente y segura.

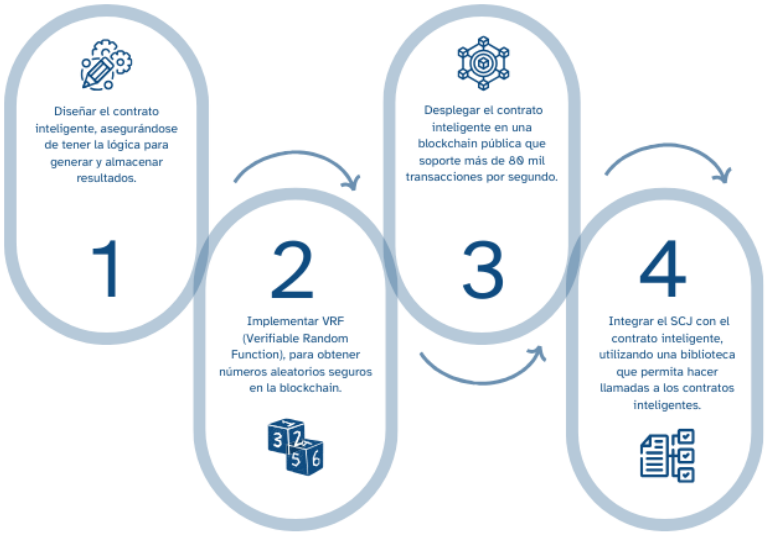
Funcionamiento de un Oráculo en Chainlink VRF

- Solicitud de Aleatoriedad: Un contrato inteligente solicita un número aleatorio llamando a la función correspondiente en Chainlink VRF.
- Generación de aleatoriedad: El oráculo genera un valor aleatorio usando una función criptográfica llamada VRF, que garantiza que el valor es impredecible y seguro.
- Prueba de Verificación: Chainlink VRF proporciona una prueba criptográfica que permite verificar que el número aleatorio fue generado de manera justa y no fue manipulado. Esta prueba se envía junto con el valor aleatorio al contrato inteligente.
- Entrega y Validación: Una vez que el valor aleatorio es recibido, el contrato inteligente puede verificar la prueba de validez para asegurarse de que el número generado es confiable. Solo entonces, el contrato puede usar ese valor aleatorio para cualquier función o lógica que dependa de la aleatoriedad.

Chainlink VRF es útil para aplicaciones que necesitan un valor aleatorio seguro, como rifas, loterías, juegos de azar, o cualquier otro que requiera decisiones al azar. Al tener un oráculo independiente que verifica la aleatoriedad, se asegura la transparencia y se evitan manipulaciones, proporcionando confianza tanto a los desarrolladores como a los usuarios de la aplicación.

En resumen, el oráculo en Chainlink VRF actúa como intermediario para generar y validar valores aleatorios de forma segura, asegurando que estos números sean confiables y demostrablemente aleatorios.

8.2. ESQUEMA DE OPERATIVIDAD Y PROCESO TÉCNICO EN LOS GNA CON SMART CONTRACTS.



Pasos para Implementación:

1. **Diseñar el Contrato Inteligente**

Diseñar el contrato para recibir números aleatorios, asegurándose de tener la lógica para generar y almacenar los resultados del juego cada vez que se invoque la función de aleatoriedad.

2. **Implementar VRF (Verifiable Random Function)**

Los contratos inteligentes deben utilizar el servicio Chainlink VRF (Función Aleatoria Verificable) para obtener números aleatorios seguros en la blockchain. El proceso sería:

- Configurar Chainlink VRF en un contrato, especificando el oráculo y las credenciales necesarias.
- Crear una función para solicitar un número aleatorio.
- El Chainlink VRF llamará a la función en el contrato cuando el número aleatorio esté disponible.
- La función generará y almacenará el número aleatorio, y posteriormente usarlo para el resultado del sorteo.

3. **Desplegar el contrato inteligente**

Una vez escrito el contrato, el siguiente paso es desplegarlo en la blockchain, cabe resaltar que debe ser una blockchain pública que soporte más de 80 mil transacciones por segundo.

Una vez desplegado, se debe guardar la dirección del contrato y el ABI (Application Binary Interface), que se necesitará para interactuar con el contrato desde el SCJ.

4. **Integrar el SCJ con el contrato inteligente**

Para la integración se debe utilizar una herramienta que permita realizar llamadas a los contratos inteligentes y realizar transacciones. Cada vez que se requiera generar un resultado para un sorteo, se interactúa con el contrato a través de la dirección del contrato que se ha desplegado.

En un entorno donde la transparencia y la confianza son esenciales, especialmente en la realización de un juego de suerte y azar, es fundamental que los participantes tengan la posibilidad de verificar los resultados de manera clara y segura, para ello, se debe construir una interfaz de usuario intuitiva y accesible que permita a cualquier persona verificar fácilmente los resultados. La interfaz mostrará de manera clara y directa los datos correspondientes a estas

transacciones, garantizando que la información provenga de la blockchain de forma segura y transparente. Esto asegura que los resultados visualizados sean fiables y verificables, aprovechando la inmutabilidad y trazabilidad que ofrece la tecnología blockchain.

5. **Información para mostrar:**

- Hash de la transacción.
- Fecha y hora de la transacción.
- Enlace directo al explorador de bloques para que los usuarios puedan verificar la transacción.
- Mostrar el número aleatorio generado.

La implementación de la tecnología blockchain en el juego de suerte y azar RIFAS, sin lugar a duda representa muchos beneficios que mejoran tanto la experiencia del usuario como la integridad y la eficiencia del sistema, la tecnología blockchain proporciona un registro de carácter público e inmutable de todas las transacciones realizadas.

Las transacciones con blockchain están aseguradas mediante criptografía avanzada, esto protege los datos de los jugadores y las transacciones de posibles ciberataques y manipulaciones; cabe mencionar que una vez que una transacción se registra en blockchain, no puede ser alterada ni eliminada, esto garantiza que todos los registros del juego de suerte y azar RIFAS sean permanentes y a prueba de manipulaciones, lo que aumenta la confiabilidad de los jugadores en la integridad del juego.

La adopción de blockchain en los juegos de suerte y azar, específicamente para la emisión de boletos y el registro del número ganador (GNA), es esencial para garantizar la transparencia y seguridad en todo el proceso. Gracias a su estructura descentralizada e inalterable, blockchain asegura que tanto las transacciones de boletos como el número ganador sean registrados de forma permanente y sin posibilidad de manipulación. Esto proporciona una protección sólida contra el fraude, permitiendo que todos los participantes tengan la certeza de que los boletos adquiridos son auténticos y que los resultados del sorteo no han sido alterados.

Cada boleto tendrá un identificador único (Código Hash) que se puede rastrear a lo largo de su ciclo de vida, esta trazabilidad asegura que solo los boletos generados a través de los canales autorizados sean válidos, impidiendo la ilegalidad y protegiendo tanto a los apostadores como a la entidad con la finalidad de generar mayor recaudo y transferencias de recursos económicos al sector de la salud.

Por esto, adoptar blockchain para la implementación del juego de suerte y azar RIFAS representa en los juegos de suerte y azar una acción innovadora y tecnológicamente avanzada, esto puede atraer la atención de muchos más jugadores que valoran la transparencia y la seguridad.

9. REQUISITOS GENERALES PARA LA COMUNICACIÓN

Se puede utilizar cualquier sistema de comunicación existente o que surja en el país, siempre y cuando se garantice la integridad de las comunicaciones entre el SCJ y todos los dispositivos de juego utilizados por la plataforma tecnológica del juego de suerte y azar RIFAS que proporcione el Operador tecnológico en su infraestructura TI.

Las Autoridades Competentes podrán establecer el detalle y las condiciones adicionales que consideren necesarias para garantizar la seguridad e integridad de las comunicaciones entre los diferentes componentes de los sistemas técnicos.

9.1. RED DE COMUNICACIONES

La red de comunicación debe ser segura para la transmisión de datos en línea. La red que utilice el Operador tecnológico, debe permitir la conectividad de todos los componentes del SCJ y todas las TDV, adicionalmente, debe poder conectarse a Internet de forma segura y a cualquier nube pública o privada que se contemple. Debe suministrarse a COLJUEGOS para su aprobación el diagrama de la red, la topología detallada de interconexión física y lógica, capacidades y estructura de la red. Los equipos de comunicaciones deben tener la capacidad de expandirse según las necesidades, y cualquier cambio sobre la red, requiere informarse a COLJUEGOS para su aprobación.

La red del SCJ deberá estar capacitada de operar con diferentes tipos de tecnología de comunicación de acuerdo con las necesidades. Además, debe ser diseñada y construida de tal manera que tenga rutas alternas (contingencia en la conectividad) en casos de problemas o interrupciones en la comunicación, tanto para los TDV e Internet como para el centro de datos con los servidores de respaldo y la réplica.

La red de comunicaciones debe tener la capacidad de transmitir transacciones al SCJ simultáneamente desde múltiples puntos de venta en internet y viceversa en línea y tiempo real, sin que esto afecte o degrade los tiempos de respuesta de las transacciones desde el momento en que el Operador tecnológico transmite la transacción hasta el momento en que inicia la impresión o generación de la boleta.

La red de comunicaciones debe tener la capacidad de entregar al SCJ la información de todos los logs que hay en la arquitectura de solución de telecomunicaciones (Dispositivos de red, oficinas de transmisión, TDV e Internet), mostrándose en un módulo de diagnóstico y con ello se puedan dar opciones de solución.

9.2. REQUISITOS PARA LOS PROTOCOLOS DE COMUNICACIÓN

Cada componente de la plataforma tecnológica del juego de suerte y azar RIFAS debe funcionar como indica el protocolo de comunicación implementado por el Operador tecnológico. El protocolo seleccionado debe utilizar técnicas de comunicación que cuenten con una apropiada detección de errores y/o mecanismos de recuperación, diseñados para prevenir intentos no autorizados de acceso o modificación. Así las cosas, el Operador tecnológico deberá contar con mecanismos que impidan accesos no autorizados y la interceptación o alteración de los datos intercambiados.

La interfaz de comunicaciones debe soportar protocolos de comunicación para la conexión de las TDV e Internet, los cuales deben garantizar la conectividad y seguridad (utilizar de guía los estándares IEEE 802 y 27001). Además, el Operador tecnológico debe asegurar como mínimo lo siguiente:

- Todas las comunicaciones críticas de datos deben fundamentarse en un protocolo, e incorporar un plan de detección de error y corrección para asegurar una precisión del 100 % sobre las transacciones recibidas.
- Todas las comunicaciones críticas de datos deben emplear un sistema de cifrado para preservar la seguridad de las comunicaciones.
- La comunicación realizada dentro del sistema debe funcionar de acuerdo a lo indicado por el protocolo de comunicación implementado.

9.3. PÉRDIDA DE COMUNICACIÓN

Cuando las comunicaciones al SCJ se han interrumpido desde la TDV o Internet, no se debe aceptar ninguna apuesta que no permita ser validada en línea con el SGR mediante conexión directa al momento de realizarla. Además, todo registro realizado en la TDV a posteriori debe ser inválido hasta que se restablezca la conectividad con el SCJ.

10.PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de las siguientes disposiciones: (i) El artículo 15 de la constitución política de Colombia que prevé que toda persona tiene derecho a *"(…) conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas, En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la constitución. (…)"* (ii) de la Ley 1581 de 2012 "*por la cual se dictan disposiciones generales para la protección de datos personales*", reglamentada parcialmente por (iii) el Decreto 1377 de 2013, y demás normas que las modifiquen, sustituyan, adicionen o complementen; y para efectos de la comercialización de juegos de suerte y azar rifas a través de las plataformas autorizadas por COLJUEGOS, el operador tecnológico de rifas, será responsable del tratamiento de datos personales conforme a la Ley aplicable.

En ese sentido se obliga a informar de manera previa al titular de los datos, al usuario o jugador el uso que se dará a los datos que suministre; así mismo, solicitará su autorización de manera previa en la plataforma para que otorgue el consentimiento previo, expreso e informado para llevar a cabo el correspondiente tratamiento de datos personales, en atención a las normas citadas sobre protección de datos personales.

Con el fin de garantizar el correcto tratamiento de los datos que los titulares, usuarios o jugadores proporcionan voluntariamente a través de la navegación en la web, el operador cumplirá sus deberes como el responsable del tratamiento de datos personales y respetará los principios rectores, derechos, demás garantías y procedimientos establecidos en la constitución y la Ley.

Todo lo anterior conforme la política de datos personales adoptada por el operador tecnológico, la cual deberá dar a conocer a sus usuarios en la plataforma de juego o en un enlace al texto de la misma, solicitando formalmente autorización para su manejo al momento de registro de cuenta de usuario y de la cual el operador se hace responsable de informar de una manera eficiente al usuario, titular o jugador de cualquier cambio modificación o adición, antes de implementar políticas nuevas, requiriendo la aceptación del usuario.

Los operadores tecnológicos deberán contar con recursos necesarios para garantizar y salvaguardar la seguridad de los registros, bases de datos, entre otros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o indebido, según la normativa vigente en materia de protección de datos.

El Operador tecnológico debe establecer los procedimientos técnicos adecuados frente a la información suministrada por el jugador, así mismo, deberá cumplir con lo previsto en las Leyes 1266 de 2008 (Habeas Data), 1480 de 2011 (Estatuto del Consumidor), 1581 de 2012 (Protección de datos Personales) y la guía de responsabilidad demostrada de la SIC: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf y cualquiera que las sustituya, modifique o adicione.

El Operador tecnológico deberá implementar las medidas de seguridad establecidas en las bases de datos y archivos según la normativa vigente en materia de protección de datos.

Será responsabilidad del Operador tecnológico la realización permanente de evaluaciones de impacto relativo a la protección de datos personales, así como la implementación de los principios de privacidad por diseño y por defecto. Dicha evaluación debe ser permanente y documentada, incluyendo los factores tenidos en cuenta, el análisis y las evaluaciones realizadas, así como las conclusiones obtenidas y las medidas implementadas para reducir y/o mitigar los riesgos identificados.

11.REQUISITOS TECNOLÓGICOS DEL SGR

11.1. RELOJ DEL SISTEMA

El reloj del sistema debe reflejar la hora actual en formato local de fecha y hora, el SGR debe ser compatible con el reloj del sistema operativo y se debe sincronizar los relojes de los servidores y los TDV. Como referencia de la hora oficial, se tendrá en cuenta la suministrada por el Instituto Nacional de Metrología - INM.

11.2. BASE DE DATOS DEL SCJ

Los servidores del SGR deben contener una base de datos de producción que almacene, en línea y en tiempo real, la información detallada de control, los resultados de los sorteos y las transacciones generadas por las TDV y los DCR a través de Internet. El sistema de gestión de bases de datos debe garantizar que sus transacciones cumplan con las características ACID (Atomicidad, Consistencia, Aislamiento, Durabilidad), asegurando su fiabilidad.

El sistema de base de datos deberá contar con funcionalidades como la realización automática de planes de mantenimiento, backups, registro de logs de transacciones y control de acceso a las tablas, así como la gestión de niveles de privilegios. Deben existir respaldos (siempre disponibles y actualizados) para garantizar el correcto funcionamiento del sistema. Además, la

información y sus datos históricos deben ser accesibles para consultas por parte de la Autoridad Competente y/o el interventor designado.

11.2.1. ACCESO A LA BASE DE DATOS

El SGR contará con mecanismos de verificación y control, que permitan la auditoría continua del sistema, evitando la modificación directa o indirecta de la base de datos. Todo el personal autorizado a operar el SCJ, mantendrá un control permanente de acceso seguro al sistema.

Las autoridades competentes y el CNJSA deben tener acceso de consulta, tanto al SGR como a la base de datos de réplica dispuesta por el operador tecnológico, con el propósito de permitirle acceder a la información correspondiente de las apuestas y registros de auditoría, como mínimo debe permitirle extraer datos de muestra del servidor de bases de datos, revisión de logs de auditoría, entre otras fuentes de información con el objetivo de poder realizar auditoría sobre los elementos enviados y registrados.

El acceso a los datos almacenados en el SGR debe ser seguro y solo a nivel de consulta, sin poner en riesgo el sistema y por consiguiente las ventas del juego.

11.2.2. INFORMACIÓN ALMACENADA EN LA BASE DE DATOS

Toda la información del SGR, su respaldo y la réplica dispuesta para las Autoridades Competentes, debe almacenar una base de datos, como mínimo, con la siguiente información:

Información Administrativa: Se refiere a la información correspondiente al Operador tecnológico del SCJ y a la información de identificación del TDV o DCR para Jugadores por Internet. Esta información debe estar almacenada en una o más bases de datos del Operador tecnológico de donde se extraerá cuando sea solicitada o consultada por la autoridad competente y el CNJSA.

Además, debe incluir como mínimo:

a) Información del Operador:

- Nit del Operador tecnológico.
- Número de contrato otorgado por la autoridad competente.
- Fecha de inicio del contrato.
- Fecha final del contrato

b) Identificación del punto de venta para TDV

- Código único del punto de venta.
- Nombre del punto de venta.
- Dirección del punto de venta.
- Barrio (Opcional).
- Municipio (Código DANE)

c) Identificación terminal de venta Fijo - Móvil

- Tipo terminal de venta (Fijo, Móvil)
- Identificación única del TDV
- Georreferenciación latitud.
- Georreferenciación longitud.
- Ubicación del municipio (Cód. DANE)
- Cód. Punto de venta asociado.

d) Identificación del jugador

- Tipo de identificación
- Número de identificación
- Primer nombre
- Segundo nombre (Opcional)
- Primer apellido
- Segundo apellido (Opcional)
- Género
- Fecha de nacimiento
- Lugar de nacimiento
- Fecha de expedición del documento de identificación
- Lugar de expedición del documento de identificación
- Fecha de vencimiento de la cédula de extranjería (Si aplica)
- Dirección de correo electrónico
- Teléfono móvil
- Georreferenciación latitud.
- Georreferenciación longitud.
- Ubicación del municipio (Cód. DANE)

Información de Control: Se refiere a los eventos significativos o sucesos generados en las TDV o desde internet o que se generan desde el SCJ como la desconexión de una TDV. Cada evento

debe ser almacenado en la base de datos del Operador tecnológico de donde se extraerá cuando sea solicitado o consultado por las autoridades competentes.

Además, debe incluir como mínimo la siguiente información:

- La fecha y hora en que ocurrió el evento.
- La identificación del TDV que generó el evento o Identificación del jugador para internet
- Un número/código exclusivo que defina el evento.
- Un texto breve que describa el evento.
- Cualquier otra información acordada con las autoridades competentes.

Información de Transacciones: Se refiere a las apuestas realizadas desde una TDV o Internet y se envían al SCJ. Cada transacción debe ser almacenada en una o más bases de datos del Operador tecnológico de donde se extraerá cuando sea solicitado o consultado por las autoridades Competentes y el CNJSA. La información de las apuestas en el SGR debe poderse identificar.

La siguiente es la información de las transacciones que debe ser transmitida en línea y tiempo real por el TDV o DCR al SGR:

- Información de cada apuesta realizada (entradas), acumulación del valor total de todas las apuestas realizadas por ubicación geográfica (municipio). El SGR mantendrá la información proporcionada por los TDV o Internet, de las apuestas realizadas, de las tablas de pago y el porcentaje de retorno de cada sorteo.
- Sorteos realizados: El SGR debe tener contadores que acumulen el número de sorteos realizados.

- Información de auditoría: Se refiere a los registros de los eventos de auditoría propios del SGR. Al momento de haber ocurrido el juego, se debe tener almacenados en una o más bases de datos información referente a las apuestas, anulaciones, resultados de los sorteos y pagos de premios. Esta información debe estar disponible cuando las Autoridades Competentes y el CNJSA lo soliciten o consulten. Deben incluir como mínimo los siguientes datos:

    - Registros en una tabla de la base de datos, la fecha, hora y tramas transmitidas diariamente hacia la réplica.

- Registros de cualquier intento de modificación o alteración de la información en la base de datos.

- Registros de las operaciones realizadas en las bases de datos, para lo cual se requerirá de un motor de bases de datos que permita realizar dicha operación automáticamente.

- Se debe garantizar, la integridad de la información almacenada en la o las bases de datos y SGR, mediante el uso de herramientas que cumplan con dicha función y garanticen el cumplimiento de controles automáticos en dichos entornos (a modo de ejemplo y sin limitar a: IBM Guardium Data Activity Monitor), igualmente la implementación de logs de auditoría en bases de datos, entre otros controles aplicables, que garanticen la trazabilidad de los cambios de un dato generado durante el tiempo. Las Autoridades Competentes y el CNJSA deberán contar con los diferentes accesos a dichas herramientas que evidencien el comportamiento de los datos a lo largo del tiempo. Será responsabilidad del operador tecnológico la implementación y gestión de dichos controles con la herramienta que se ajuste a su solución tecnológica.

El software de administración y configuración del SGR no debe permitir acceso a usuarios no registrados (utilizar como guía los estándares ISO/IEC 27001).

12.REQUISITOS DE SEGURIDAD

El SGR y su respaldo (contingencia) podrán estar en nubes públicas. El SGR puede estar en la misma nube que el respaldo, o en una nube diferente. La réplica deberá permanecer ubicada en un Data Center con características mínimas de TIER III o superior en territorio colombiano. Cabe aclarar que, las Autoridades Competentes y el CNJSA podrán acceder tanto a la réplica como al SGR y su contingencia cuando lo desee mediante una VPN y cómo las Autoridades Competentes y el CNJSA dispongan.

La plataforma tecnológica que soporta el sistema debe cumplir mínimo con los siguientes requisitos de seguridad (utilizar como guía el estándar de ISO/IEC 27001):

- La transmisión de la información se debe realizar utilizando un sistema que garantice la privacidad de los datos que son transportados dentro de la red.
- Debe contener un módulo de auditoría.

- Se debe garantizar la efectividad, eficiencia, confidencialidad, integridad, disponibilidad y cumplimiento de la información que se transmite entre las TDV, DCR para Internet y el SGR.
- La información de los eventos de control, de resultados y de apuestas almacenada en el SGR debe conservarse en las bases de datos o en respaldos históricos durante la vigencia del contrato más dos (2) años adicionales.
- Se deben implementar las funciones de auditoría y trazabilidad en el motor de base de datos que permita identificar e individualizar todos los movimientos y transacciones en la base de datos.

- El SGR no permitirá modificar la información que se obtenga desde el TDV o el DCR para internet y debe notificar al administrador del sistema y bloquear al usuario de la TDV o al jugador para internet, tras un número fijo de intentos de ingreso frustrados.
- El SGR debe ser diseñado para proteger la integridad de los datos importantes en la eventualidad de una falla.
- Los registros de auditoría, base de datos del sistema, y cualquier otro dato importante deben ser almacenados utilizando métodos de protección razonables.
- Cumplir con condiciones de seguridad tanto física como lógica que impidan accesos no autorizados al software y a las bases de datos.
- Proteger las claves de acceso a los sistemas de información, bases de datos, sistemas operativos y jugadores. En desarrollo de esta obligación, el Operador tecnológico debe evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de los establecimientos autorizados debe ser única y personalizada.
- Si se utilizan discos duros como medio de almacenamiento, se debe asegurar la integridad de los datos en el evento de una falla del disco. Los métodos aceptables incluirán, pero no estarán limitados a múltiples discos duros en una configuración aceptable RAID, o réplica/duplicado de datos entre dos o más discos duros, el método utilizado debe proporcionar también un soporte abierto para copias de seguridad y restablecimiento.
- La implementación del esquema de copia de seguridad debe ocurrir al menos una vez todos los días. Debe asegurar el poder restaurar de forma segura la información de 5 años atrás.
- Manejo y seguridad de los medios de almacenamiento que deben ser informados a las Autoridades Competentes
- Requisitos para la Recuperación: En el evento de una falla catastrófica, cuando el SGR no pueda ser reiniciado de ninguna otra forma, debe ser posible volver a cargar la base de

datos desde el último punto de copia de seguridad viable, y recuperar totalmente los contenidos de esa copia de seguridad; principalmente con la siguiente información:

- Eventos significativos
- Información de auditoría
- Información del sitio específico como la configuración del juego, cuentas de seguridad, etc.

12.1. ACCESO A LA CONFIGURACIÓN DEL JUEGO

El SGR no debe permitir acceso a usuarios no registrados (se utiliza como guía los estándares ISO/IEC 27001), debe generar los registros de acceso y modificación en la información de auditoría.

Protección Contra Intrusiones: Todos los servidores tendrán la suficiente protección física/lógica contra accesos no autorizados, debe generar los registros correspondientes en la información de auditoría en caso de presentarse este evento.

Requisitos del Acceso a la Configuración: El menú de configuración/instalación del SGR no debe estar disponible para personal no autorizado y debe contar con un método de acceso seguro.

Programación del Servidor: No debe haber medios disponibles para que un Operador tecnológico lleve a cabo una programación en el servidor que permita modificar la base de datos de resultados de los eventos y las transacciones generadas en los TDV o los DCR para Internet.

Protección contra Virus: Todos los servidores, TDV y dispositivos del SCJ deben contar con una protección contra virus licenciada o su equivalente.

Protección contra copias: Disponer de una protección contra copias, para prevenir la proliferación no autorizada o modificación del software, para servidores o TDV. Su implementación debe incluir:

- Documentación total del método
- Posibilidad de verificación individual de cualquier dispositivo envuelto en hacer cumplir la protección contra copias.

12.2. CONTROL DE ACCESO

El SGR debe contar o con una estructura jerárquica de personificación por la cual el nombre del usuario y la contraseña definen el acceso a los programas y a las opciones, en particular de menús, o bien admitirá el acceso a programas y dispositivos de forma segura, basándose estrictamente en el nombre del usuario y contraseña. Se puede fortalecer la seguridad del acceso remoto, por medio de un elemento de soporte físico (*hardware*) y una firma digital que autentifique y garantice el acceso autorizado (verificación en 2 pasos). El SGR no debe permitir ninguna alteración del registro de información que haya sido comunicada desde la TDV o el DCR para internet. Además, debe existir la funcionalidad para notificar al administrador o generar el registro de auditoría correspondiente, cuando ocurra un número determinado de intentos de entradas de acceso fracasadas y bloqueo de usuario o jugador.

Asimismo, debe cumplir mínimo con las siguientes condiciones:

- El Operador tecnológico debe establecer un protocolo de acceso físico y lógico a sus sistemas técnicos de juego en el que se recojan los procedimientos para su control, la relación de las personas que dispongan de autorización para el acceso, así como las operaciones que pueden realizar en los sistemas.
- El registro de acceso al SGR y a la base de datos en la réplica debe ser conservado por el Operador durante la ejecución del contrato y dos años (2) adicionales a su terminación.
- El SGR y la base de datos en la réplica deben ser accesibles únicamente por las personas expresamente designadas por el Operador a estos efectos, y en el marco de una inspección, por el personal de las autoridades competentes.
- El Operador tecnológico debe establecer las medidas de seguridad físicas y lógicas que aseguren el control del acceso a los sistemas técnicos, que impidan el acceso y permitan la detección de cualquier persona no autorizada.
- El Operador tecnológico debe realizar, mínimo una vez al año, pruebas de vulnerabilidad a los diferentes sistemas y plataformas de información utilizada para la operación del juego, documentar los resultados y generar el plan de mitigación pertinente. Todos estos documentos deben ser informados a las autoridades competentes.
- Inclusión del concepto de seguridad en la definición de roles y perfiles del personal.
- Gestión, control, registro y seguimiento del acceso a usuarios del sistema.
- Control, registro y seguimiento de acceso a redes, sistema operativo y aplicaciones.
- Seguridad en el desarrollo y mantenimiento de los sistemas.

12.3. SEGURIDAD EN EL SISTEMA DE COMUNICACIÓN

Todas las comunicaciones entre los componentes del SCJ, incluido cualquier acceso remoto, deben pasar a través de por lo menos un cortafuego (firewall) a nivel aplicación (application-level) aprobado y no tendrá la facilidad de permitir una ruta de red alterna. Si existe una ruta de red alterna para propósitos de redundancia, esta también debe pasar a través de por lo menos un cortafuego (firewall) a nivel aplicación (application-level).

Esta aplicación de cortafuegos (firewall) debe mantener un registro de auditoría de la siguiente información, y debe desactivar todas las comunicaciones y generar un evento de error si el registro de auditoría se llena en su totalidad:

- Todos los cambios de configuración del cortafuego (firewall).
- Todos los intentos de conexión exitosos o fallidos hechos a través del cortafuego (firewall).
- Direcciones IP de la fuente y destino, y número de puerto.

El registro deberá estar disponible cuando las Autoridades Competentes lo soliciten o consulten.

12.4. SEGURIDAD EN EL ACCESO REMOTO

El acceso remoto es definido como cualquier acceso al SGR desde fuera del sistema de red confiable. El acceso al SGR en forma remota debe cumplir con las mínimas condiciones de seguridad exigidas, como lo son el uso de firewall lógico o físico, VPN, usuario y contraseña (utilizar como guía el estándar ISO/IEC 27001). Para el caso de acceso remoto seguro por internet, éste debe ser seguro, fiable y apropiado a sus aplicaciones, utilizando para ello la encriptación SSL estándar y la tecnología de navegación web para solucionar los problemas de acceso sin tener requisitos de entorno del usuario o jugador. De los accesos al SGR se debe registrar la información que permita posteriormente realizar un seguimiento de un evento ocurrido. El acceso remoto debe cumplir con siguientes requisitos:

- Generar el registro de la actividad de los usuarios por acceso remoto, que describa el nombre del usuario, la fecha y hora, duración y la actividad desarrollada durante el acceso.
- No se deben permitir funcionalidades administrativas por usuarios remotos sin autorización (por ejemplo, agregando usuarios, cambiando permisos, etc.)
- No se debe permitir el acceso a la base de datos sin autorización.
- No se debe permitir el acceso al sistema operativo sin autorización.

- No se deben realizar sesiones remotas sin que se genera la grabación de esta.
- Si la base de datos del acceso remoto es constante, se debe instalar un filtro de red (firewall) o un sistema diseñado para prevenir el acceso de usuarios no autorizados y proteger la información de ataques externos.

- Auditoría de Acceso Remoto: El sistema central debe mantener un registro de actividad ya sea automáticamente, o permitiendo el ingreso manual de dicho registro, describiendo toda información de acceso remoto que incluya:

    - Nombre de acceso
    - Tiempo y fecha de cuando la conexión fue realizada
    - Duración de la conexión
    - Actividad mientras está registrado, incluyendo el acceso a áreas específicas y cambios que fueron realizados.

NOTA: Se reconoce que el fabricante del SCJ podrá acceder de forma remota al sistema y a sus componentes asociados con el propósito de soportar la solución. Sin embargo, este acceso debe ser autorizado, grabado y realizado por un medio seguro. Este registro debe estar disponible cuando las Autoridades Competentes lo soliciten o consulten.

12.5. ALTERACIÓN DE DATOS

El SGR no permitirá la alteración de la información de control, ni de transacciones transmitidas desde los TDV o DCR para internet. Si por alguna razón se modifica esta información, se debe generar un registro automático de auditoría con la siguiente información:

- Dato alterado.
- Valor del dato previo a la alteración.
- Valor del dato después de la alteración.
- Hora y fecha de la alteración.
- Usuario que realizó la alteración (usuario activo en el SGR)

Se debe garantizar, la integridad de la información almacenada en la o las bases de datos y SGR, mediante el uso de herramientas que cumplen con dicha función y garantizan el cumplimiento de controles automáticos en dichos entornos (a modo de ejemplo y sin limitar a: IBM Guardium,

Data Activity Monitor), igualmente la implementación de logs de auditoría en bases de datos, entre otros controles aplicables, que garanticen la trazabilidad de los cambios de un dato generado durante el tiempo. Las Autoridades Competentes y el CNJSA deberán contar con los diferentes accesos a dichas herramientas que evidencien el comportamiento de los datos a lo largo del tiempo. Será responsabilidad del operador tecnológico la implementación y gestión de dichos controles con la herramienta que se ajuste a su solución tecnológica.

Este registro debe estar disponible cuando las Autoridades Competentes lo soliciten o consulten.

12.6. CONTROL DEL SISTEMA CENTRAL DEL JUEGO.

Los siguientes componentes del SCJ y su respaldo (contingencia) podrán estar en nubes públicas. El SCJ puede estar en la misma nube que el respaldo, o en una nube diferente.

- Software de Gestión de RIFAS - SGR
- Software de Validación de Apuestas
- Software de Generación de Sorteos - GNA
- Software de capa media y Hardware de Almacenamiento

El SCJ en sus diferentes componentes, así como su sistema de respaldo, incorporarán conexiones informáticas seguras, que permitan realizar un control y seguimiento, en tiempo real si así se requiriera, de la actividad de juego llevada a cabo, de la venta de boletas y premios otorgados, todo ello sin perjuicio de la posibilidad de realizar inspecciones presenciales.

Corresponde al Operador tecnológico el mantenimiento de una VPN que permita el acceso de las Autoridades Competentes al SGR y a su respaldo, garantizando la actualización en línea y tiempo real de las bases de datos ahí contenidas.

12.7. COPIAS DE RESPALDO Y RECUPERACIÓN

El Operador tecnológico debe garantizar la existencia de copias redundantes de cada archivo de registro o base de datos del sistema o ambos en el SGR con soporte abierto para las copias de seguridad y recuperación (se refiere al estándar ISO/IEC 27001).

12.8. REQUISITOS PARA LA RECUPERACIÓN

En caso de un fallo del SGR el sistema debe tener la capacidad de recargarse desde las copias de seguridad, recuperando plenamente los contenidos en un plazo no mayor a doce (12) horas. Se recomienda que se incluya como mínimo la siguiente información:

- Información de auditoría.
- Información administrativa.
- Información de control.
- Información financiera (ventas y pagos).

El SGR no debe permitir la modificación o alteración de ninguna información de control o contadores que haya sido comunicado desde el TDV o DCR para internet, conservando la trazabilidad de cualquier intento de modificación o alteración en los registros del SGR (utilizar como guía el estándar ISO/IEC 27001).

13. REGISTRO, TRAZABILIDAD DE LAS OPERACIONES DE JUEGO Y LA BASE DE DATOS

- El SGR debe garantizar la trazabilidad y el registro de la totalidad de las operaciones de juego y de las transacciones económicas que se realicen, permitiendo la reconstrucción fiel de los sorteos y las transacciones realizadas: apuestas realizadas, ganadoras, pagadas, no pagadas y anuladas.
- El SGR realizará la captura, registro y conservación de las transacciones.
- Todos los elementos del SCJ deben estar protegidos física y lógicamente e impedir cualquier acceso no autorizado.

El Operador tecnológico también debe incluir en la base de datos segura:

- Los datos de control mínimos establecidos por las Autoridades Competentes.
- Un registro de eventos que incluya al menos las interrupciones del servicio o inhabilitación de juegos.
- Cualquier otro dato requerido por las Autoridades Competentes de forma general o individual en un procedimiento de control.

- La base de datos segura y los registros del Operador deben conservarse por un período mínimo de la vigencia del contrato más dos años (2) adicionales, debiéndose establecer los sistemas de protección y respaldo que aseguren su integridad y seguridad durante ese plazo, así como su recuperación íntegra ante eventualidades.

13.1. CONTINUIDAD DE LA ACTIVIDAD DE JUEGO

El Operador debe diseñar e implementar un DRP ("*Disaster Recovery Plan*") cuyos protocolos deben ser seguidos en caso de falla de la plataforma tecnológica y por lo tanto del SCJ con el objetivo de recuperar el sistema mediante los planes de contingencia establecidos en un plazo no mayor a doce (12) horas. Es importante aclarar que, la disponibilidad del servicio contratado al año para la solución debe ser del 99,982%, es decir: 8,758.43horas. Por consiguiente, la indisponibilidad permitida es de 8,760 horas−8,758.43 horas = **1.57 horas**. Ahora, se puntualiza que el tiempo máximo para recuperar la operación (DRP) la cual está contemplada tanto en Hardware como en Software será de doce (12) horas.

Este DRP debe garantizar la continuidad de la operación del juego, la recuperación de la data debe estar garantizada. El operador tecnológico debe presentar a Coljuegos para su aprobación tanto el DRP como los resultados de las pruebas regulares realizadas sobre este el mismo.

Especificar que el sistema central de juego y el respaldo deben estar en al menos 2 zonas diferentes de la nube pública elegida por el operador.

Adicionalmente, el Operador tecnológico debe disponer de un plan de contingencia tecnológica que cumpla con lo siguiente:

- Contemplar las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio. El Operador debe informar adecuadamente sobre sus políticas en relación con las interrupciones del servicio y la forma en que los clientes pueden verse afectados. El Operador debe adoptar las medidas necesarias para garantizar que sus clientes reciban un trato justo en caso de interrupción del juego o la realización de apuestas.
- Garantizar que, en ningún caso, se pierdan datos o transacciones que afecten o puedan llegar a afectar el desarrollo de los juegos, a los derechos de los participantes, o al interés público.
- COLJUEGOS evaluará el plan de contingencia tecnológica y, en su caso, requerirá al Operador la adopción de las medidas adicionales que considere precisas para asegurar la continuidad de las actividades del juego.
- El Operador tecnológico debe realizar por lo menos un simulacro al año de este plan de contingencia y verificación de cumplimiento de lo establecido en el DRP, dicho proceso debe ser avalado por COLJUEGOS y/o el interventor designado.

14. ASPECTOS ADMINISTRATIVOS

Asegurar la puesta en funcionamiento de la totalidad del Sistema del juego de suerte y azar RIFAS, para lo cual es necesario que se tengan implementados por lo menos los siguientes procesos, los cuales corresponden a las mejores prácticas de administración de sistemas (se utiliza como guía el estándar ISO/IEC 9001):

- Administración de niveles y continuidad del servicio
- Administración de los servicios de terceros
- Administración del desempeño y capacidad
- Administración de la seguridad de los sistemas
- Educación y entrenamiento a los usuarios
- Administración de la configuración
- Administración de los problemas
- Administración de los datos
- Administración del ambiente físico
- Administración de las operaciones
- Procedimientos a seguir cuando se evidencia alteración o manipulación de las máquinas o información.

15. ESPECIFICACIONES TÉCNICAS PARA LA INFORMACIÓN ALMACENADA EN EL SGR Y LA RÉPLICA.

A continuación, se describen los datos mínimos que debe tener el SGR y la réplica dispuesta a las autoridades Competentes, en cumplimiento de las obligaciones establecidas en el contrato de concesión para operar las RIFAS. COLJUEGOS se reserva el derecho a solicitar modificar, adicionar o eliminar campos específicos de las tablas reportadas por el Operador tecnológico en la Base de Datos en la réplica, los cuales serán informados oportunamente al Operador tecnológico para que este realice los cambios correspondientes.

La actualización de esta información ante las autoridades competentes, es independiente de otras solicitudes de informes que se soliciten al Operador para efectos de control del juego.

15.1. CONDICIONES GENERALES DE LA RÉPLICA

- El Operador debe siempre generar una réplica exacta de la Base de Datos del SGR del juego de suerte y azar RIFAS en el Data Center TIER III. Se debe tener en cuenta la

necesidad de sistemas Master-Slave (Maestro-Esclavo) en la solución en caso que así se requiera para la réplica.

- Toda transacción generada sobre las diferentes tablas de la base de datos del Sistema Central del Juego debe ser replicada en línea sobre la base de datos ubicada en el sistema de réplica con el objetivo de garantizar la integridad de la misma y permitir el seguimiento a la entidad.
- El Operador tecnológico debe entregar en medio digital a la autoridad competente y/o el interventor designado los siguientes documentos al inicio del proyecto, y cada vez que sean modificados para su respectiva validación y aprobación:

    - Diccionario de datos de todas las tablas que componen la estructura de la base de datos.
    - Diagrama Entidad - Relación y Modelo Relacional.
    - Toda la documentación relacionada con los objetos de la base de datos.

15.2. ESPECIFICACIONES DE INFORMACIÓN

A continuación, se describe la información mínima que el Operador tecnológico debe incluir en la base de datos del SGR y, por consiguiente, en la réplica ubicada en el TIER III. Le corresponde al Operador tecnológico especificar la estructura de las tablas para la réplica de información a las Autoridades Competentes agregando como mínimo, las tablas y campos estipulados en el diseño de referencia del modelo de datos, y conforme a las condiciones generales indicadas en el numeral anterior.

Todos los campos descritos a continuación son de obligatorio diligenciamiento.

15.2.1. INFORMACIÓN DEL OPERADOR

IDENTIFICACIÓN DEL OPERADOR	
Dato	Lista de Valores
nit_operador	Número de Identificación tributaria del operador autorizado
numero_contrato	Número del contrato otorgado por la Autoridad Competente (Si aplica)
acto_administrativo	Número de la resolución de autorización emitida por la autoridad competente.
fecha_inicio_contrato	Fecha de inicio del contrato (Si aplica).
fecha_fin_contrato	Fecha fin del contrato (Si aplica).

15.2.2. IDENTIFICACIÓN PUNTO DE VENTA PARA TDV

IDENTIFICACIÓN PUNTO DE VENTA (No aplica para internet)	
Dato	Lista de Valores
id	Identificador único del punto de venta.
cod_tdv	Código único la terminal de venta
nombre	Nombre del punto de venta.
dirección	Dirección del punto de venta
barrio	Barrio del punto de venta (Opcional)
cod_municipio	Código del municipio del punto de venta según DIVIPOLA
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.

15.2.3. IDENTIFICACIÓN DEL TERMINAL DE VENTA FIJO O MÓVIL

IDENTIFICACIÓN TERMINAL DE VENTA	
Dato	Lista de Valores
id	Identificación única del terminal en el sistema cuando sea fijo o móvil.
cod_tdv	Código único la terminal de venta
georef_latitud	Georreferenciación latitud. Si es tipo móvil, se registra la ubicación del vendedor o usuario
georef_longitud	Georreferenciación longitud. Si es tipo móvil, se registra la ubicación del vendedor o usuario
estado_tdv	Estado de la terminal de venta (Activa, Inactiva)
tipo	Tipo de terminal (Fijo, Móvil)
id_punto_de_venta	Identificador del punto de venta
cod_municipio	Código del municipio según DIVIPOLA
nit_propietario	Identificación del propietario de la TDV
propietario_tdv	Razón social del propietario de la TDV
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.

15.2.4. IDENTIFICACIÓN DEL JUGADOR (Aplica para Internet)

IDENTIFICACIÓN DEL JUGADOR	
Dato	Lista de Valores
id	Identificador único del usuario.
tipo_documento	Tipo de documento del usuario. • Cédula de ciudadanía para ciudadanos colombianos. • Cédula de extranjería vigente en su condición de visa, expedida por el Estado Colombiano para ciudadanos extranjeros. • Pasaporte • Permiso Especial de Permanencia (PEP) • Permiso Especial de Permanencia para el Fomento de la Formalización (PEPFF) • NIT • y demás documentos que autorice el gobierno nacional.
documento	Número de documento del usuario.
fecha_expedicion	Fecha de expedición del documento (Debe ser inferior a la fecha de creación del usuario)
lugar_expedicion	Lugar de expedición del documento (Código de municipio según divipola)
fecha_expiracion	Fecha de expiración del documento, aplica para CE, PPT y PEP
primer_nombre	Primer nombre del usuario.
segundo_nombre	Segundo nombre del usuario (si aplica).
primer_apellido	Primer apellido del usuario.
segundo_apellido	Segundo apellido del usuario (si aplica).
telefono	Teléfono de contacto del usuario.
dirección_de_residencia	Dirección del usuario.
genero	Género registrado en el documento de identidad
fecha_nacimiento	Fecha de nacimiento del usuario
lugar_nacimiento	Lugar de nacimiento del usuario (código municipio divipola)
correo	Dirección de correo electrónico
cod_departamento	Código del departamento según los códigos establecidos por el DANE (DIVIPOLA)

IDENTIFICACIÓN DEL JUGADOR	
Dato	Lista de Valores
cod_ciudad	Código de la ciudad según los códigos establecidos por el DANE (DIVIPOLA)
password	Contraseña encriptada del usuario
ruta_certificado_representacion_legal	Ruta del archivo del certificado de representación legal (si aplica)
estado	Estado de la cuenta del usuario A: Activo I: Inactivo
id_grupos_usuarios	Identificador del grupo de usuarios al que pertenece
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.
deleted_at	Fecha y hora de eliminación (si aplica).

15.2.5. INFORMACIÓN DE EVENTOS POR USUARIO

IDENTIFICACIÓN EVENTOS POR USUARIO	
Dato	Lista de Valores
id	Identificador del evento
id_usuario	Identificador del usuario
cod_evento	Código del evento ocurrido (Cambio de estado, etc…).
descripcion	Descripción del evento ocurrido
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.

15.2.6. INFORMACIÓN DE LA VENTA (APUESTAS)

INFORMACIÓN DE LA VENTA (Apuestas)	
Dato	Lista de Valores
id	Identificador único de la venta.
id_usuario	Identificador del usuario que realizó la compra. FK - Relacionado con scj_usuarios
id_rifa	Identificador de la rifa asociada a la venta. FK - Relacionado con scj_rifas
id_transaccion	Identificador de la transacción asociada a la venta. FK - Relacionado con scj_transacciones

INFORMACIÓN DE LA VENTA (Apuestas)	
Dato	Lista de Valores
id_boleto	Identificador del boleto vendido. FK - Relacionado con scj_boletos
valor_boleta_con_iva	Valor de boleta con IVA.
valor_boleta_sin_iva	Valor de boleta sin IVA
Valor_iva	Valor del IVA de lo apostado en el boleto
created_at	Fecha y hora de creación del registro de la venta.

15.2.7. INFORMACIÓN DE MEDIOS DE PAGO

INFORMACIÓN DE LOS MEDIOS DE PAGO	
Dato	Lista de Valores
id	Identificador único del medio de pago.
Nombre	Nombre del medio de pago (por ejemplo, tarjeta de crédito, transferencia, etc.).
corto	Nombre corto del método de pago EF: Pagos en efectivo a través de puntos físicos establecidos por el Operador Para Internet: BC: Cuentas bancarias en entidades autorizadas CR: Tarjeta de crédito. IN: Instrumento de pago ofrecido por entidad vigilada por la Superintendencia Financiera de Colombia GI: Transferencia de giro PR: Tarjeta prepago recargable OT: Otro medio de pago ofrecido por el Operador.
estado	Estado del medio de pago (activo, inactivo).
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.

15.2.8. INFORMACIÓN DE LOS SORTEOS

INFORMACIÓN SORTEO

Dato	Lista de Valores
id	Identificador único de la rifa.
id_usuario	Identificador del usuario responsable de la rifa
nombre_rifa	Nombre de la rifa que se realizará y su registro ante el respectivo operador autorizado por la autoridad competente.
numero_acto_administrativo	Número del acto administrativo que autoriza la realización de la rifa
ruta_acto_administrativo	Ruta al documento del acto administrativo que autoriza la realización de la rifa
fecha_acto_administrativo	Fecha del acto administrativo que autoriza la realización de la rifa
hora_acto_administrativo	Hora del acto administrativo que autoriza la realización de la rifa
cc_representante_legal	Ruta a copia de cédula del representante legal
certificado_existencia_representacion_legal	Ruta a certificado de existencia y representación legal
tipo_de_sorteo	GNA o Lotería
loteria_del_sorteo	Nombre de la lotería que realizará el sorteo (Sí el tipo de sorteo es “Lotería”, este campo aplica)
lugar_sorteo	
fecha_hora_apertura	Fecha y hora de apertura de la rifa.
fecha_hora_cierre	Fecha y hora de cierre de la rifa.
fecha_hora_rifa	Fecha y hora en que se realiza el sorteo.
estado	Estado de la rifa (activa, cerrada, etc.).
valor_boleta_con_iva	Valor de venta al público de cada tiquete y/o boleta electrónica con IVA.

valor_boleta_sin_iva	Valor de venta al público de cada tiquete y/o boleta electrónica IVA.
cantidad_boletas	Número de tiquetes y/o boletas electrónicas que dan derecho a participar en la rifa.
hash_transaccion_blockchain_sorteo	Hash de la transacción en la blockchain.
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.
deleted_at	Fecha y hora de eliminación (si aplica).

15.2.9. INFORMACIÓN DE BOLETOS

INFORMACIÓN DE BOLETOS	
Dato	Lista de Valores
id	Identificador único del boleto.
numero_apuesta	Número de la apuesta.
código_hash	Código hash único asociado al boleto.
estado	Estado del boleto (vendido, reservado, no vendido, anulado, ganador, etc.).
id_blockchain_boleto	Identificación de la tabla scj_blockchain_boleto
metadatos_adicionales	Metadatos adicionales asociados al boleto.
hash_boleto	Hash asociado al boleto
created_at	Fecha y hora de creación del boleto.
updated_at	Fecha y hora de la última actualización.

15.2.10. INFORMACIÓN DE BOLETOS POR RIFA

INFORMACIÓN DE BOLETOS	
Dato	Lista de Valores
id	Identificador único del boleto.
id_rifa	Identificador de la rifa a la que pertenece este boleto
id_boleto	Identificador del boleto
created_at	Fecha y hora de creación del boleto.

INFORMACIÓN DE BOLETOS	
Dato	Lista de Valores
updated_at	Fecha y hora de la última actualización.

15.2.11. INFORMACIÓN DE BOLETOS EN BLOCKCHAIN

INFORMACIÓN DE BOLETOS EN BLOCKCHAIN	
Dato	Lista de Valores
id	Identificador único del blockchain boleto.
id_blockchain	Identificador de la cadena de bloques
fecha_firma_blockchain	Fecha y hora de la firma en blockchain
registro_anchor	Registro anchor
id_anchor	Identificador del registro anchor
estado_anchor	Estado de anchor
ruta_pdf	Ruta al archivo pdf (si aplica)
hash_pdf	Hash del archivo pdf
altura_block	Altura del bloque
ruta_ots	Ruta del archivo OTS (si aplica).
hash_ots	Hash del archivo OTS para validación.
firma	Prueba de firma del boleto en la blockchain.
created_at	Fecha y hora de creación del boleto.
updated_at	Fecha y hora de la última actualización.

15.2.12. INFORMACIÓN DE GANADORES POR RIFA

INFORMACIÓN DE GANADORES POR RIFA	
Dato	Lista de Valores
id	Identificador único del ganador.
id_rifa	Identificador de la rifa en la que ganó el usuario.
id_boleto	Identificador del boleto ganador.
combinacion_ganadora	Número del boleto ganador
Id_usuario	Identificador del usuario ganador
id_transaccion_blockchain	Identificador o hash de la transacción en blockchain
id_premio	Identificador del premio
estado	Indica el estado en el que se encuentra la entrega del premio

INFORMACIÓN DE GANADORES POR RIFA	
Dato	Lista de Valores
fecha_entrega	Fecha de entrega del premio
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.

15.2.13. INFORMACIÓN DE TRANSACCIONES

INFORMACIÓN DE TRANSACCIONES	
Dato	Lista de Valores
id	Identificador único de la transacción.
fecha_pago	Fecha del pago de la transacción.
hora_pago	Hora del pago de la transacción.
codigo_unico	Código único de la transacción.
id_tdv	Identificación del terminal de venta (TDV).
valor_total_transaccion_con_iva	Valor total de la transacción con IVA.
valor_total_transaccion_sin_iva	Valor total de la transacción sin IVA.
id_medio_pago	Identificador del medio de pago.
tipo_transaccion	Tipo de transacción realizada
estado	Estado de la transacción (pendiente, completada, etc.).
cod_municipio	Código del municipio (DIVIPOLA) en el que se encuentra el usuario al momento de la compra
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.

15.2.14. INFORMACIÓN DE DERECHOS DE EXPLOTACIÓN

INFORMACIÓN DE BOLETOS	
Dato	Lista de Valores
id	Identificador único del derecho de explotación.
id_entidad_territorial	Identificador de la entidad territorial asociada al derecho.
id_transaccion	Identificador de la transacción asociada al derecho de explotación.
valor_total_pagado	Valor total pagado por derechos de explotación (dato no lleva IVA)
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.

15.2.15. INFORMACIÓN DE ENTIDADES TERRITORIALES

INFORMACIÓN DE ENTIDADES TERRITORIALES	
Dato	Lista de Valores
id	Identificador único de la entidad territorial.
nombre	Nombre de la entidad territorial
cuenta_bancaria	Cuenta bancaria asociada a la entidad territorial
tipo_cuenta	Tipo de cuenta en la entidad bancaria
entidad_bancaria	Nombre de la entidad bancaria
estado	Estado de la entidad territorial
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.

15.2.16. INFORMACIÓN DE LOS PREMIOS

INFORMACIÓN DE ENTIDADES TERRITORIALES	
Dato	Lista de Valores
id	Identificador único de la entidad territorial.
nombre	Nombre de la entidad territorial
cuenta_bancaria	Cuenta bancaria asociada a la entidad territorial
id	Identificador único del premio
id_rifa	Id de la rifa a la que pertenece el premio
nombre	Nombre que se le da al premio
descripcion	Descripción completa del premio
adjuntos	Ruta a los archivos adjuntos asociados al premio
orden	Orden o peso del premio (1, 2, 3, etc.)
valor_premio	Valor en pesos colombianos del premio
Fecha_caducidad	Fecha de caducidad del premio
created_at	Fecha y hora de creación del registro.
updated_at	Fecha y hora de la última actualización.

15.2.17. RESULTADOS DEL JUEGO POR SORTEO

El operador del juego de suerte y azar RIFAS debe garantizar que se encuentre la información necesaria en la Base de Datos para generar con periodicidad diaria y mensual el siguiente reporte:

RESULTADOS TOTALES POR SORTEO	
Dato	Lista de Valores
Número Sorteo	Número consecutivo por sorteo realizado
Número Tiquetes Válidos	Número Tiquetes Válidos
Número Tiquetes Anulados	Número Tiquetes Anulados
Cantidad Ganadores	Cantidad Ganadores
Total Premio Ganadores	Valor bruto del premio, sin retenciones

15.2.18. REPORTE DE INGRESOS BRUTOS POR TERMINAL DE VENTA

El operador del juego de suerte y azar RIFAS debe garantizar que se encuentre la información necesaria en la Base de Datos para generar con periodicidad diaria y mensual el siguiente reporte:

INGRESOS TERMINAL DE VENTA	
Dato	Lista de Valores
Identificación Única Terminal de Venta	Identificación del terminal en el Sistema Central del Juego
Código Punto de Venta	Código definido por el Operador al momento de realizar su proceso de despliegue.
Código del sorteo	Código definido por el operador para la identificación única de cada sorteo.
Ventas Totales sin IVA Sorteo 1	Valor bruto de apuestas recaudadas en 1er sorteo del día
Valor Total Premios Pagados Sorteo 1	Valor bruto de premios pagados sin retenciones 1er sorteo del día
Cantidad Premios Pagados Sorteo 1	Total número de premios pagados en 1er sorteo del día

15.2.19. REPORTE DE PREMIOS POR TIQUETE

El operador del juego de suerte y azar RIFAS debe garantizar que se encuentre la información necesaria en la Base de Datos para generar con periodicidad diaria y mensual el siguiente reporte:

REPORTE PREMIOS POR TIQUETE	
Dato	Lista de Valores
Número Sorteo	Número consecutivo por sorteo realizado
Código hash de seguridad de la venta	Código hash único asociado al boleto.
Fecha Venta de Tiquete	Fecha en que se realizó la venta del tiquete
Combinación Ganadora	Número del boleto ganador
Valor Premio	Valor del premio
Estado Premio	Lista de valores estado de premio: • Pagado • Por pagar • Prescrito
Fecha Pago Premio	Fecha definida para el pago de los premios.

16. ESPECIFICACIONES TÉCNICAS DE LA CONSULTA DE INFORMACIÓN PARA LAS AUTORIDADES COMPETENTES Y EL CNJSA

A continuación, se describe lo que debe disponer el operador tecnológico para permitir a las autoridades competentes y al CNJSA realizar consultas y reportes de información, en cumplimiento de las obligaciones establecidas en el contrato de concesión para operar las RIFAS. Las especificaciones de este documento y aquellos que formen parte integral de la reglamentación del juego de suerte y azar RIFAS, serán modificadas por COLJUEGOS en caso de que la Entidad considere necesario, e informadas oportunamente al Operador tecnológico para que este garantice su operación.

16.1. GENERADOR DE REPORTES

- El operador tecnológico dispondrá para las autoridades competentes de una herramienta de usuario final para generar reportes personalizados en adelante denominada "Generador de reportes".
- El Generador de reportes se debe conectar en línea y tiempo real a la información de la base de datos del SGR réplica dispuesta en el Data Center TIER III. Por medio de un usuario de consulta podrá generar reportes de manera dinámica con la información especificada en el numeral "15.2. ESPECIFICACIONES DE INFORMACIÓN" de este documento.

- El Generador de reportes debe permitir seleccionar uno o varios datos de una o varias tablas del SGR que se requieran para la generación de un reporte con esta selección, permitiendo al usuario de las Autoridades Competentes y al CNJSA disponer de un reporte personalizado. Este reporte podrá exportarse en un archivo plano delimitado por comas y/o PDF de tal forma que se tenga mayor flexibilidad en la generación de la información.
- El operador tecnológico debe entregar a las Autoridades Competentes y al CNJSA el procedimiento para la solicitud del usuario de consulta del Generador de reportes, donde indique mínimo como se debe solicitar este usuario.
- El operador tecnológico proporcionará a las autoridades competentes y al CNJSA el manual de usuario del Generador de reportes, el cual contiene la guía de instrucciones que sirve para el uso del generador de reportes y el procedimiento o solución de problemas.
- El operador tecnológico garantizará que el usuario solicitado por las autoridades competentes y el CNJSA sólo tendrá acceso de consulta a la información especificada en el numeral **"15.2 ESPECIFICACIONES DE INFORMACIÓN"** de este documento, que cumpla con las mejores prácticas del ciclo de vida de un usuario y asegure la custodia de estas credenciales de una forma controlada y responsable.
- El sistema de generación de reportes debe tener la capacidad de operar de manera indistinta, a elección de la entidad sobre las bases de datos o sistemas de información del SGR o sobre la información del sistema de réplica. Dicha selección de fuentes de información debe ser de uso fácil y sencillo para el usuario final.

16.1.1. REPORTES DE INFORMACIÓN FINANCIERA

Los reportes financieros del SGR corresponden a la administración de los recursos económicos derivados de la operación de las rifas. Su implementación debe garantizar la trazabilidad de cada transacción, asegurando la integridad de la información y el cumplimiento de las normativas establecidas. Estos reportes deben ofrecer herramientas de control, automatización y validación que permitan una gestión eficiente y transparente de los recursos.

En lo que respecta a la liquidación, el sistema debe operar bajo modelos de recaudo referenciado, permitiendo la identificación automática de cada transacción y su registro inmediato en la plataforma. Además, debe contar con herramientas que faciliten el monitoreo de pagos y la generación de reportes detallados en tiempo real.

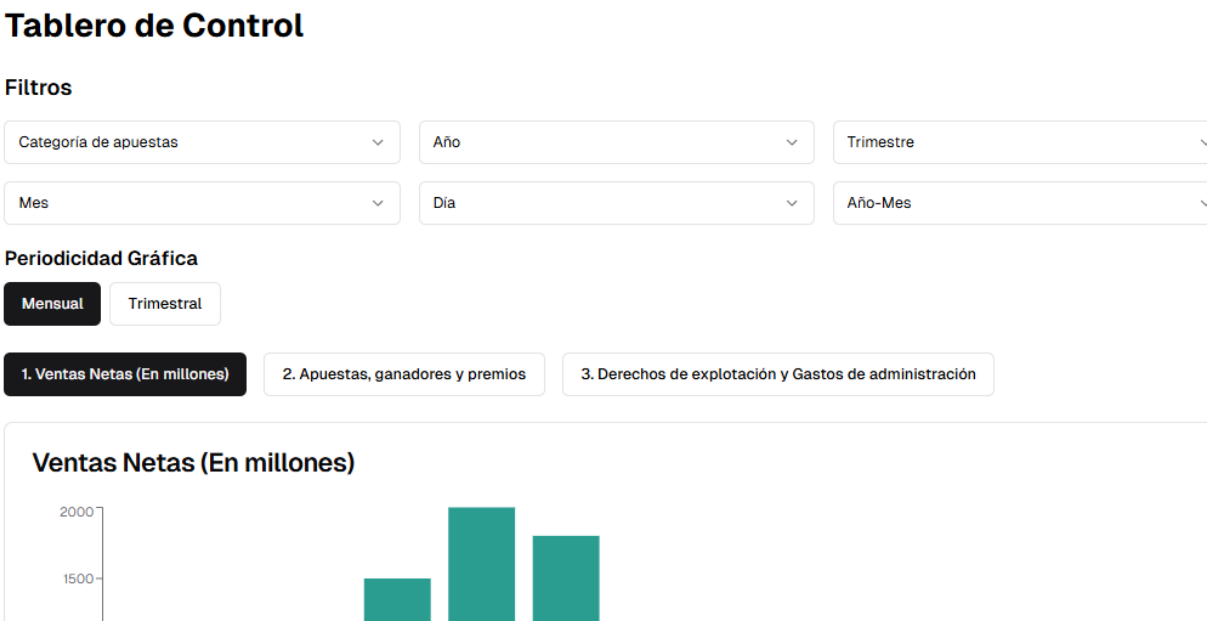
Cada uno de estos procesos dentro de los aspectos financieros debe ser diseñado bajo una arquitectura de alta disponibilidad y seguridad, permitiendo la verificación en tiempo real de cada transacción y posibilitando la generación de reportes para las autoridades competentes. El

cumplimiento estricto de estas funcionalidades garantizará la transparencia operativa y el control eficiente de los recursos financieros.

16.2. TABLERO DE CONTROL

- El operador tecnológico dispondrá en su SGR de "Tableros de control" (Dashboard) que permitan generar información estadística de ventas, apuestas, número de ganadores, premios, derechos de explotación y gastos de administración, por sorteo (para todas las mecánicas de acuerdo con el decreto 1486 del 2024) y con las fechas de corte deseadas, desde la fecha de inicio de acto administrativo de autorización hasta el corte del mes inmediatamente anterior a la fecha de consulta.
- Este Tablero de control debe consultar en línea y tiempo real los datos registrados en la base de datos de la Réplica para generación de la información estadística.
- El operador tecnológico debe entregar a las autoridades competentes el procedimiento para la solicitud del usuario de consulta del Tablero de control, donde indique mínimo como se debe solicitar este usuario y quien debe solicitarlo.
- El operador tecnológico proporcionará a las autoridades competentes y al CNJSA el manual de usuario del Tablero de control, el cual contiene la guía de instrucciones que sirve para su uso y el procedimiento o solución de problemas.
- El operador tecnológico garantizará que el usuario solicitado por las autoridades competentes y el CNJSA sólo tendrá acceso al Tablero de Control, que cumpla con las mejores prácticas del ciclo de vida de un usuario y asegure la custodia de estas credenciales de una forma controlada y responsable.
- El tablero de control debe tener la capacidad de operar de manera indistinta, a elección de la entidad sobre las bases de datos o sistemas de información del SGR o sobre la Réplica. Dicha selección de fuentes de información debe ser de uso fácil y sencillo para el usuario final designado por las Autoridades Competentes y el CNJSA.
- Permitir exportar los datos en Excel de la información de generada para los tableros de control.
- El operador tecnológico deberá proporcionar todos los tableros de acuerdo a las específicas técnicas establecidas por las Autoridades Competentes.

16.2.1. ESPECIFICACIÓN FUNCIONAL



El **Tablero de control** debe tener una sección en donde por medio de botones se seleccionan los filtros para la información a la cual se le generan las estadísticas.

Filtros

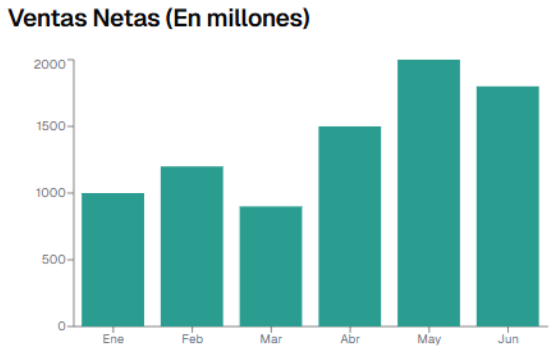
- **Combinación ganadora** (De acuerdo con el decreto del juego)
- **Año, Trimestre, Mes, Día, Año-Mes**
- **De acuerdo con el filtro seleccionado** (Periodicidad Gráfica).
- **Ubicación geográfica** (TDV, Ventas, usuarios, premios entregados, entre otros)
- **Puntos de ventas**
- **Tipo de Tiquete** (Físico o Electrónico)
- **Sorteos**
- **Número de contrato**
- **Autoridades competentes**

El Tablero de control debe tener tres botones con los cuales permiten generar las estadísticas gráficas y valores:

Ventas Netas (En millones)

Apuestas, ganadores y premios

Derechos de explotación y Gastos de administración.



Resumen de Ventas Netas

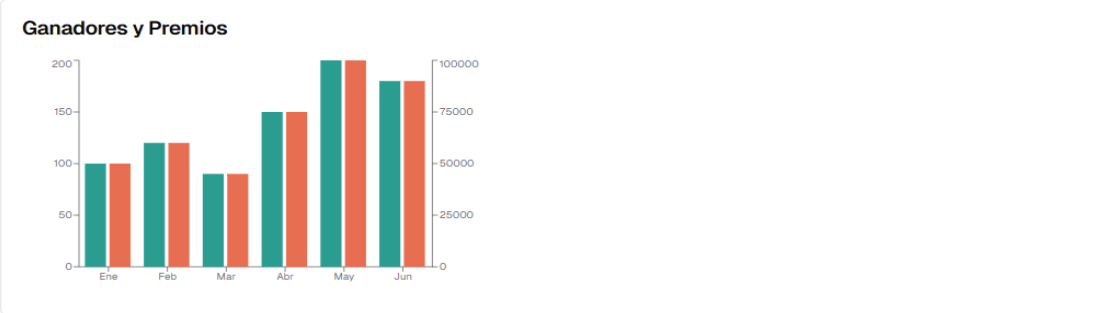
Métrica	Valor Completo	Valor en Millones
Total Periodo	8400	0.01
Promedio Trimestral	2800	0.00

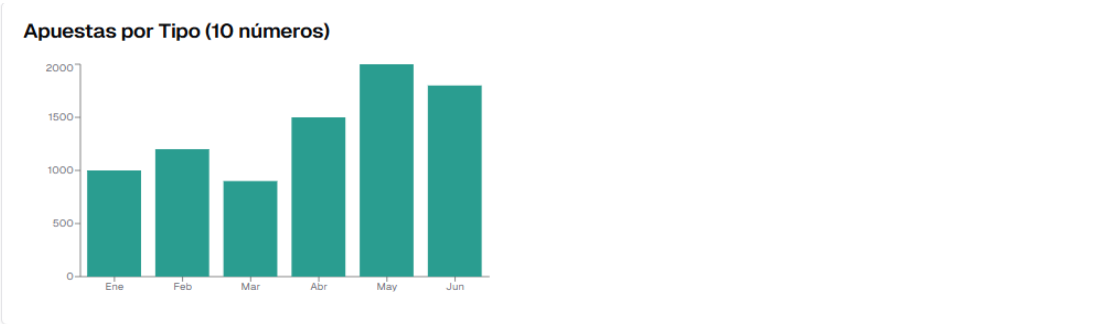
De acuerdo con los filtros seleccionados al dar Clic en el botón **1. Ventas Netas (En millones)**, se deben generar las estadísticas gráficas y tabla con los valores de acuerdo con los filtros de las fechas y periodos seleccionados.

Se presenta la gráfica de acuerdo con el filtro seleccionado en "Periodicidad gráfica", totalizando por los filtros de las fechas y periodos seleccionados con la **cantidad de ventas netas** respectivas.

En una tabla, de acuerdo con los filtros de las fechas y periodos seleccionados, se presentan los valores completos y los valores en millones, así:

- **TOTAL PERÍODO**
- **PROMEDIO TRIMESTRAL**
- **PROMEDIO MENSUAL**
- **PROMEDIO DÍAS CON SORTEOS**





Resumen de Apuestas, Ganadores y Premios

Métrica	Apuestas	Ganadores	Premios
Total Periodo	8400	840	420.000
Promedio Trimestral	2800	280	140.000

De acuerdo con los filtros seleccionados al dar Clic en el botón **2. Apuestas, ganadores y premios**, se deben generar las estadísticas gráficas y tabla con los valores de acuerdo con los filtros de las fechas y periodos seleccionados.

Se presenta la gráfica de acuerdo con el filtro seleccionado en "Periodicidad gráfica" (Trimestral y Mensual), totalizando por los filtros de las fechas y periodos seleccionados para:

- **Cantidad de ganadores**
- **Valor premios de la cantidad de ganadores**

Se presenta la gráfica de acuerdo con el filtro seleccionado en "Periodicidad gráfica" (Trimestral y Mensual), totalizando por los filtros de las fechas y periodos seleccionados para tipo de apuesta.

En una tabla de acuerdo con filtros de las fechas y periodos seleccionados se presentan los valores completos y los valores en millones para **APUESTAS, GANADORES y PREMIOS**

POR PERIODO, PROMEDIO TRIMESTRAL, PROMEDIO MENSUAL y PROMEDIO DÍAS CON SORTEOS.

Resumen de Derechos de Explotación y Gastos de Administración

Métrica	Derechos de Explotación (D.E.)	Gastos de Administración (G.A.)	D.E. + G.A.
Total Periodo	840	420	1260
Promedio Trimestral	280	140	420
Promedio Mensual	140	70	210
Promedio Días con Sorteos	28	14	42

De acuerdo con los filtros seleccionados al dar Clic en el botón **Derechos de explotación y Gastos de administración**, se deben generar las estadísticas gráficas y tabla con los valores de acuerdo con los filtros de las fechas y periodos seleccionados.

Se presenta la gráfica de acuerdo con el filtro seleccionado en "Periodicidad gráfica" (Trimestral y Mensual), totalizando por los filtros de las fechas y periodos seleccionados para:

- **Total ventas**
- **Valor suma Derechos de explotación más Gastos de administración**

Los Derechos de explotación y los Gastos de administración se calculan de acuerdo con la reglamentación vigente.

En una tabla de acuerdo con filtros de las fechas y periodos seleccionados se presentan los valores completos y los valores en millones para: **DERECHOS EXPLOTACIÓN (D.E.), GASTOS DE ADMINISTRACIÓN (G.A.) y D.E. + G.A. POR TOTAL PERIODO, PROMEDIO TRIMESTRAL, PROMEDIO MENSUAL** y **PROMEDIO DÍAS CON SORTEOS.**

Cabe resaltar que lo expuesto para los tableros de control y tablas en el presente anexo se encuentra sujetos a los cambios, actualizaciones, modificaciones y peticiones adicionales que sean de consideración de las Autoridades Competentes.

17. CERTIFICACIÓN

El tercero interesado en acreditarse como Operador tecnológico deberá someter su SCJ ante un laboratorio certificador avalado por COLJUEGOS y/o por quien haga sus veces para que éste realice las pruebas necesarias y le otorgue una certificación en idioma español del cumplimiento de los Requerimientos Técnicos indicados en el presente documento. Dicha certificación debe ser enviada por el operador tecnológico dentro del plazo definido por Coljuegos y CNJSA para su verificación y validación. En todo caso, Coljuegos previo a la acreditación del Operador tecnológico verificará el cumplimiento de los requerimientos técnicos exigidos para el SCJ a nivel de funcionamiento.

El laboratorio y/o quien haga sus veces conforme a lo dispuesto por Coljuegos debe realizar ensayos de seguridad, cumplimiento y funcionalidad, basados en los requisitos indicados en el presente documento y cualesquiera otros requisitos técnicos desarrollados de acuerdo con las funcionalidades y especificaciones del producto del operador autorizado, con la finalidad de garantizar la integridad y transparencia de la operación de los equipos y software que son parte de la solución tecnológica.

Los ensayos al SCJ del juego de suerte y azar RIFAS pueden ser efectuados en las instalaciones del laboratorio o en las instalaciones del proveedor del sistema. El laboratorio debe realizar las pruebas al sistema en conjunto con las TDV con el equipo ensamblado y con los DCR para internet, y también en campo donde la instalación y comunicación será probada antes de su implementación.

Cualquier modificación o actualización que implique algún cambio en el SCJ certificado por el laboratorio, deberá ser sometida a un proceso de control de calidad y validación por parte del ente certificador previo a su puesta en operación o producción. En todo caso, los costos asociados a la certificación estarán a cargo del Operador tecnológico.

Esta certificación tendrá una validez de doce (12) meses. Previo al vencimiento del plazo, el operador deberá solicitar un proceso de recertificación en la misma forma, tiempo y lugar que la certificación inicial, con el fin de verificar el cumplimiento de todos los requisitos técnicos y operativos para el adecuado funcionamiento del SCJ.

Cada re-certificación deberá ser presentada a COLJUEGOS como ente acreditador del Operador tecnológico, dentro de los quince (15) días hábiles antes del inicio de cada año de operación.

18. GESTIÓN DE TICKETS Y MESA DE AYUDA DEL SISTEMA

La gestión eficiente de soporte técnico es un componente esencial en la operatividad del SCJ. Debe existir una mesa de ayuda que garantice tiempos de respuesta óptimos, resuelva incidentes de manera efectiva y mantenga un registro detallado de cada solicitud para asegurar la mejora continua del sistema. El proceso de gestión de tickets debe seguir un flujo estructurado para minimizar el impacto de incidencias y proporcionar una experiencia de soporte ágil y eficiente.

- **Recepción y Clasificación de Incidencias*:*** El proceso inicia con la recepción del ticket a través de los diferentes canales habilitados, como un portal web de soporte, correo electrónico, chatbot o llamadas telefónicas. Al recibir la solicitud, el sistema debe asignar automáticamente un número de ticket y clasificar la incidencia según su tipo y nivel de prioridad:
    - Incidencias críticas: Problemas que afectan la operación del sistema en su totalidad o impiden el acceso de los usuarios.
    - Errores funcionales: Fallos que afectan ciertas funciones, pero no impiden completamente la operación.
    - Consultas generales: Dudas sobre el uso del sistema o procesos administrativos.
- **Asignación y Priorización:** Los tickets deben ser asignados al equipo de soporte adecuado según la categoría y complejidad del problema. Para los casos de alta prioridad, se debe activar un protocolo de respuesta inmediata con escalamiento a los equipos de desarrollo si es necesario.
- **Diagnóstico y Resolución:** El equipo de soporte analizará el problema y proporcionará una solución dentro de los tiempos de respuesta definidos según sea establecido internamente por el Operador Tecnológico en sus acuerdos de nivel de servicio (SLA). Dependiendo de la naturaleza de la incidencia, se pueden aplicar soluciones temporales hasta que se implemente una solución definitiva en el sistema.

- **Pruebas y Validación de la Solución:** Antes de cerrar el ticket, se debe validar la solución aplicada, asegurando que el problema ha sido completamente resuelto y que no genera nuevas incidencias. En algunos casos, se pueden requerir pruebas de usuario para verificar la funcionalidad restaurada.
- **Cierre y Documentación:** Una vez confirmada la solución, el ticket se marca como resuelto y se genera un informe detallado con la descripción del problema, acciones tomadas y recomendaciones para evitar futuras incidencias. Esta documentación servirá para análisis posteriores y mejora continua.
- **Seguimiento y Evaluación de Servicio:** Para garantizar la calidad del soporte, se deben realizar encuestas de satisfacción tras la resolución de cada ticket. Además, se pueden establecer métricas clave de desempeño, como tiempo medio de resolución, tasa de reabiertos y volumen de tickets gestionados, con el fin de optimizar el servicio.

19. MODIFICACIONES

La determinación de los requisitos y condiciones, por su característica fundamentalmente tecnológica, pueden estar sujetos a cambios derivados de la innovación tecnológica.

Coljuegos se reserva todas las facultades para definir el detalle de los procedimientos, requisitos y condiciones técnicas que, por su misma naturaleza, puedan estar sujetos a cambios derivados de la innovación tecnológica.

Los nuevos desarrollos en la tecnología implementada y los requerimientos adicionales que el Operador solicite a los fabricantes deben ser compatibles con los requisitos mínimos contemplados en este documento.

El operador tecnológico podrá proponer, para aprobación de las Autoridades Competentes, mejoras a los requerimientos técnicos para la operación del juego, con observancia de los siguientes aspectos:

1. Se conservan las características del juego descritas en el reglamento del juego.
2. Se garantice que se mantienen las condiciones mínimas establecidas en el presente documento, sin poner en riesgo la seguridad técnica y operativa del juego.