

(CNJSA), para que suscriba del acto administrativo conjunto con la Empresa Industrial y Comercial del Estado (Coljuegos), mediante el cual se expiden los “REQUERIMIENTOS TÉCNICOS DEL SISTEMA PARA LA OPERACIÓN DEL JUEGO DE SUERTE Y AZAR RIFAS” de conformidad con lo establecido en los artículos 1° y 12 del Decreto número 1486 de 2024, que modificó el Decreto número 1068 de 2015.

Que la presente resolución fue publicada en el sitio web de Coljuegos y del Consejo Nacional de Juegos de Suerte y Azar (CNJSA) desde el 21 de julio de 2025 hasta el 1° de agosto de 2025, con el fin de que los interesados pudieran presentar las observaciones y comentarios que consideraran pertinentes. Todos los aportes recibidos fueron analizados por Coljuegos y por la Secretaría Técnica del Consejo Nacional de Juegos de Suerte y Azar (CNJSA), y aquellos que se consideraron viables fueron incorporados al documento.

Que, en mérito de lo expuesto,

RESUELVE:

Artículo 1°. *Objeto.* Expedir de manera conjunta entre Coljuegos y el Consejo Nacional de Juegos de Suerte y Azar (CNJSA), el Anexo de Requerimientos Técnicos para la operación del Juego de Suerte y Azar en la modalidad de Rifas, el cual hace parte integral de la presente resolución.

Artículo 2°. *Autorización de terceros operadores tecnológicos en el juego de suerte y azar rifas.* Coljuegos será el responsable de autorizar a los terceros interesados en actuar como operadores tecnológicos en el juego de suerte y azar en la modalidad de rifas, previa verificación del cumplimiento de los Requerimientos Técnicos contenidos en el Anexo al que hace referencia el artículo primero de la presente resolución.

Las obligaciones técnicas a cargo de los operadores tecnológicos autorizados serán las previstas en el Anexo de Requerimientos Técnicos para la operación del Juego de Suerte y Azar en la modalidad de Rifas, que hace parte de la presente resolución, así como del acto administrativo de autorización que expida Coljuegos.

Parágrafo: Las autoridades competentes para autorizar la realización de rifas a terceros gestores de acuerdo con el territorio donde se comercialice, son cada una de las entidades territoriales o Nacional, según corresponda, conforme a lo previsto en el artículo 2.7.3.3 del Decreto número 1068 de 2015. Las autoridades competentes deberán identificar plenamente en los actos administrativos de autorización de las rifas, el operador tecnológico a través del cual se llevará a cabo la rifa.

Artículo 3°. *Certificación sistema central de juego.* Establecer, conforme a lo dispuesto en el Anexo de Requerimientos Técnicos para la operación del juego de suerte y azar en la modalidad de rifas que en cada trámite de autorización a un tercero operador tecnológico, se le otorgará por parte de las autoridades competentes, un plazo máximo de seis (6) meses, contados a partir de la ejecutoria del acto administrativo de autorización, para que estos acrediten la certificación del Sistema Central de Juego.

Artículo 4°. *Periodo de transición.* Establecer en concordancia del artículo 12 del Decreto número 1486 de 2024, que los operadores y/o gestores de juegos de rifas contarán con un término de doce (12) meses contados a partir de la entrada en vigencia del presente acto administrativo mediante el cual se expiden los requerimientos técnicos para que ajusten sus plataformas tecnológicas y sistemas de información de acuerdo con lo exigido en los Requerimientos Técnicos que corresponden al anexo del presente acto administrativo.

Durante dicho periodo, los terceros interesados en ser operadores tecnológicos podrán ajustar sus plataformas tecnológicas y sistemas de información de acuerdo con lo exigido en los mencionados Requerimientos Técnicos para presentar las solicitudes de autorización. Así mismo, mientras persista dicho periodo, las autoridades competentes para autorizar rifas, podrán aprobar a los gestores la comercialización del juego con boletas físicas y de manera manual. Los requisitos serán los previstos en el reglamento y bajo el procedimiento que disponga cada autoridad competente. En este caso, los resultados contra los cuales se cursarán las rifas de comercialización manual serán los definidos en el numeral 1 del artículo 2.7.3.4 de este reglamento, es decir, los resultados del premio mayor de las Loterías tradicionales que operen legalmente en Colombia,

Artículo 5°. *Ámbito de aplicación.* La presente resolución aplica a las personas jurídicas en calidad de operadores tecnológicos que soliciten autorización ante Coljuegos conforme lo definido en el presente Acto Administrativo.

Artículo 6°. La presente resolución rige a partir de su publicación en el *Diario Oficial*.

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 11 de agosto de 2025.

La Presidente del CNJSA,

Flor Esther Salazar Guatibonza.

El Presidente Coljuegos,

Marco Emilio Hincapié Ramírez.

Folios: tres (3)

Anexos: Anexo de Requerimientos Técnicos para la operación del Juego de Suerte y Azar en la modalidad de Rifas. Nombre y número de expediente: 20161200710100001E - Actos Administrativos de carácter general.

ANEXOS:

Anexo de Requerimientos Técnicos para la operación del Juego de Suerte y Azar en la modalidad de Rifas.

Coljuegos

CNJSA

CONSEJO NACIONAL DE JUEGOS DE SUERTE Y AZAR

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

JULIO 2025

OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN.

Hacienda

CNJSA

Coljuegos

CONSEJO NACIONAL DE JUEGOS DE SUERTE Y AZAR

Tabla de contenido

GLOSARIO

OBJETIVO

CONSIDERACIONES

Contenido

1. ASPECTOS TÉCNICOS GENERALES 13

2. REQUISITOS TECNOLÓGICOS DE FUNCIONALIDAD DEL SCJ.18

2.1. SISTEMA DE CONTROL PARA ALTOS FLUJOS DE TRANSACCIONES....22

2.2. TRANSMISIÓN DE SORTEOS MEDIANTE USO DE HERRAMIENTAS TECNOLÓGICAS-STREAMING.22

3. GESTIÓN DE LAS RIFAS23

3.1. ROLES EN EL PROCESO23

3.2. REGISTRO DE GESTORES24

3.3. SOFTWARE DE GESTIÓN DE RIFAS (CREACIÓN Y AUTORIZACIÓN)..25

3.3.1. MÓDULO DE AUTORIZACIÓN25

3.3.1.1. SUBMÓDULO DE CREACIÓN DE UNA RIFA.....25

3.3.1.2. SUBMÓDULO DE GESTIÓN DE DOCUMENTOS.26

3.3.1.3. SUBMÓDULO DE LIQUIDACIÓN28

3.3.1.4. SUBMÓDULO DE PAGO28

3.3.1.5. SUBMÓDULO DE PROCESO DE NOTIFICACIÓN (AUTORIZACIÓN)28

3.3.2. MÓDULO DE COMERCIALIZACIÓN.....29

3.3.2.1. REGISTRO DEL APOSTADOR EN EL CANAL DE VENTA POR INTERNET.....30

3.3.2.2. CIERRE DE COMERCIALIZACIÓN Y PROCESO DE RELIQUIDACIÓN (DEVOLUCIÓN)”.34

3.3.4. VERIFICACIÓN DE GANADOR37

3.3.4.1. VERIFICACIÓN DE LA.ENTREGA DEL PREMIO38

4. DESARROLLO DEL SOFTWARE GESTIÓN DE RIFAS (SGR).39

5. HARDWARE Y SOFTWARE DISPUESTO PARA LAS AUTORIDADES COMPETENTES40

5.1. REQUISITOS GENERALES DE LA TERMINAL DE VENTA - TDV40

5.2. REQUISITOS DE IDENTIFICACIÓN DE LA TERMINAL DE VENTA - TDV42

5.2.1. IMPRESORA DE BOLETAS42

5.2.2. DISPOSITIVOS DE CONEXIÓN REMOTA - DCR.....42

6. VENTA DE BOLETAS43

Página 2 de 93

 6.1. GENERACIÓN DEL boletas ELECTRÓNICas43 7. TECNOLOGÍA BLOCKCHAIN PARA LA EMISIÓN DE BOLETOS.45 7.1. ESQUEMA DE OPERATIVIDAD Y PROCESO TÉCNICO EN LA EMISIÓN DE BOLETOS.47 7.2. VERIFICACIÓN DE BOLETOS CON BLOCKCHAIN.....49 8. REQUISITOS GENERALES DE FUNCIONALIDAD PARA EL GNA50 8.1. TECNOLOGÍA BLOCKCHAIN PARA GNA51 8.2. ESQUEMA DE OPERATIVIDAD Y PROCESO TÉCNICO EN LOS GNA CON SMART CONTRACTS.53 9. REQUISITOS GENERALES PARA LA COMUNICACIÓN56 9.1. RED DE COMUNICACIONES.....56 9.2. REQUISITOS PARA LOS PROTOCOLOS DE COMUNICACIÓN57 9.3. PÉRDIDA DE COMUNICACIÓN57 10. PROTECCIÓN DE DATOS PERSONALES.....58 11. REQUISITOS TECNOLÓGICOS DEL SGR 59 11.1. RELOJ DEL SISTEMA59 11.2. BASE DE DATOS DEL SCJ59 11.2.1. ACCESO A LA BASE DE DATOS.....60 11.2.2. INFORMACIÓN ALMACENADA EN LA BASE DE DATOS.....60 12. REQUISITOS DE SEGURIDAD 63 12.1. ACCESO A LA CONFIGURACIÓN DEL JUEGO65 12.2. CONTROL DE ACCESO66 12.3. SEGURIDAD EN EL SISTEMA DE COMUNICACIÓN.....67 12.4. SEGURIDAD EN EL ACCESO REMOTO.....67 12.5. ALTERACIÓN DE DATOS.....68 12.6. CONTROL DEL SISTEMA CENTRAL DEL JUEGO.....69 12.7. COPIAS DE RESPALDO Y RECUPERACIÓN69 12.8. REQUISITOS PARA LA RECUPERACIÓN.....70 13. REGISTRO, TRAZABILIDAD DE LAS OPERACIONES DE JUEGO Y LA BASE DE DATOS.....70 13.1. CONTINUIDAD DE LA ACTIVIDAD DE JUEGO71 14. ASPECTOS ADMINISTRATIVOS 72 15. ESPECIFICACIONES TÉCNICAS PARA LA INFORMACIÓN ALMACENADA EN EL SGR Y LA RÉPLICA. 72 15.1. CONDICIONES GENERALES de la réplica.....72 15.2. ESPECIFICACIONES DE INFORMACIÓN.....73 15.2.1. INFORMACIÓN DEL OPERADOR.....73 15.2.2. IDENTIFICACIÓN PUNTO DE VENTA PARA TDV.....74 15.2.3. IDENTIFICACIÓN DEL TERMINAL DE VENTA FIJO O MÓVIL.....74 15.2.4. IDENTIFICACIÓN DEL JUGADOR (Aplica para Internet).....75  Página 3 de 93 www.coljuegos.gov.co	 15.2.5. INFORMACIÓN DE EVENTOS POR USUARIO 76 15.2.6. INFORMACIÓN DE LA VENTA (APUESTAS) 76 15.2.7. INFORMACIÓN DE MEDIOS DE PAGO 77 15.2.8. INFORMACIÓN DE LOS SORTEOS 77 15.2.9. INFORMACIÓN DE BOLETOS 79 15.2.10. INFORMACIÓN DE BOLETOS POR RIFA..... 79 15.2.11. INFORMACIÓN DE BOLETOS EN BLOCKCHAIN..... 80 15.2.12. INFORMACIÓN DE GANADORES POR RIFA 80 15.2.13. INFORMACIÓN DE TRANSACCIONES..... 81 15.2.14. INFORMACIÓN DE DERECHOS DE EXPLOTACIÓN 81 15.2.15. INFORMACIÓN DE ENTIDADES TERRITORIALES 81 15.2.16. INFORMACIÓN DE LOS PREMIOS 82 15.2.17. RESULTADOS DEL JUEGO POR SORTEO 82 15.2.18. REPORTE DE INGRESOS BRUTOS POR TERMINAL DE VENTA 83 15.2.19. REPORTE DE PREMIOS POR TIQUETE..... 83 16. ESPECIFICACIONES TÉCNICAS DE LA CONSULTA DE INFORMACIÓN PARA LAS AUTORIDADES COMPETENTES y el CNJSA.. 84 16.1. GENERADOR DE REPORTES.....84 16.2. TABLERO DE CONTROL86 16.2.1. ESPECIFICACIÓN FUNCIONAL 87 17. CERTIFICACIÓN..... 91 18. GESTIÓN DE TICKETS Y MESA DE AYUDA DEL SISTEMA..... 92 19. MODIFICACIONES..... 93  Página 4 de 93 www.coljuegos.gov.co
 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. 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  Página 5 de 93 www.coljuegos.gov.co	 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  Página 6 de 93 www.coljuegos.gov.co



www.collegesiskiyous.gov.co



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.	Municipio
Operación en dos (2) o más municipios del mismo departamento.	Gobernación o Sociedad de Capital Público Departamental
Operación en un (1) municipio de un departamento y en el Distrito Capital.	
Operación en dos (2) o más municipios de diferentes departamentos.	
Operación en un 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 con el 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:

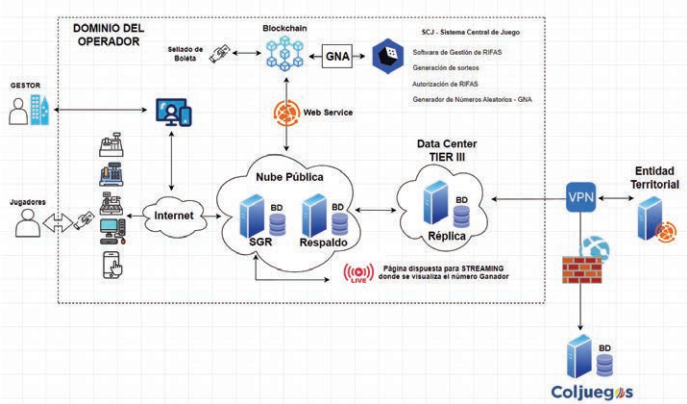


Ilustración 1. Fuente: Coljuegos.

Las Autoridades Competentes y el 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.

Hacienda CNJSA Coljuegos 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: A. 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 y/o Oracle, 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 Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos 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, de uso, de usuario y toda aquella documentación, entre otra y sin limitar a: diagramas físicos (a modo de ejemplo: Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos 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 transmisión 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 estructurados, 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 transmisión 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 Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos 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. Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos	Hacienda CNJSA Coljuegos 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, de uso, de usuario y toda aquella documentación, entre otra y sin limitar a: diagramas físicos (a modo de ejemplo: Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos 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 transmisión 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 estructurados, 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 transmisión 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 Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos 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. Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos
Hacienda CNJSA Coljuegos 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 transmisión 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 estructurados, 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 transmisión 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 Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos	Hacienda CNJSA Coljuegos 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. Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos Hacienda CNJSA Coljuegos



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 garanticen 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 in 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 de consulta 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 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 los números ganadores, 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

 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 (Opcional) • 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 • Dirección de residencia • 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.  Página 31 de 93 www.coljuegos.gov.co	 • 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, complementen 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 boleto. • Disponer de los medios de pago para realizar la compra de las apuestas, como lo son:  Página 32 de 93 www.coljuegos.gov.co
 - Transferencias desde cuentas bancarias. - Tarjetas débito o crédito avaladas y emitidas por entidades autorizadas y vigiladas por la Superintendencia Financiera de Colombia. - Cualquier otro medio de pago de los autorizados por la Superintendencia Financiera de Colombia. - 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 en todos los canales de comercialización. 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  Página 33 de 93 www.coljuegos.gov.co	 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. En ambos casos el SGR permitirá al gestor generar un informe de la totalidad de las boletas emitidas identificando cuales números fueron vendidos y/o reportados como no disponibles por encontrarse invalidados y cuales no fueron vendidos, informe que deberá enviar al correo registrado al momento de la creación del usuario por la autoridad competente y el CNJSA según corresponda, a más tardar el día hábil anterior a la fecha de realización del sorteo. 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.  Página 34 de 93 www.coljuegos.gov.co

 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  Página 39 de 93 	 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.  Página 40 de 93 
 - 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:  Página 41 de 93 	 - 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 tickets 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  Página 42 de 93 



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 ticket 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 ticket, 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, haciendo uso de cualquiera de las tres formas de verificación dispuestas por el operador tecnológico.

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.

6UHkSF763

Verificar

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.

Suelte aquí el archivo o haga clic para cargarlo

Seleccionar

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 ticket 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.

Información registrada en Blockchain.

Hash del 87623ymkxgfr6y634i2o3u4jhr6y4y2
Metadata: 7dfdf334
Bloque: 987342
Tipo de registro: BTCOpReturn
Fecha de firma en Blockchain: 19-02-2024 04:04:33 Pm
[Link de Blockchain](#)

Archivos de Blockchain.

Proof
Descargar
Opentimestamp
Descargar Verificar

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

Hacienda CNJSA Coljuegos

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 tickets 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:

Página 51 de 93

Hacienda CNJSA Coljuegos

- 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. 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

Página 52 de 93

Hacienda CNJSA Coljuegos

- **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.

Página 53 de 93

Hacienda CNJSA Coljuegos

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

Página 54 de 93



El Operador tecnológico y/o Gestor (como responsable o encargado según corresponda) 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 y/o Gestor (como responsable o encargado según corresponda) 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 y/o gestor (como responsable o encargado según corresponda) 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

Página 59 de 93

www.coljuegos.gov.co



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.

Página 60 de 93

www.coljuegos.gov.co



- 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 o DCR

- 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.

Página 61 de 93

www.coljuegos.gov.co



- 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, 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:

Página 62 de 93

www.coljuegos.gov.co

 • 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):  Página 63 de 93 	 • 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.  Página 64 de 93 
 • 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. <u>Protección Contra Intrusiones:</u> 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. <u>Requisitos del Acceso a la Configuración:</u> El menú de configuración/instalación del SGR no debe estar disponible para personal no autorizado y debe contar con un método de acceso seguro. <u>Programación del Servidor:</u> 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. <u>Protección contra Virus:</u> Todos los servidores, TDV y dispositivos del SCJ deben contar con una protección contra virus licenciada o su equivalente. <u>Protección contra copias:</u> 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  Página 65 de 93 	 • 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 (<i>hardware</i>) y una firma digital que autentique 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.  Página 66 de 93 

 • 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.)  Página 67 de 93 www.coljuegos.gov.co	 • 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)  Página 68 de 93 www.coljuegos.gov.co
 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).  Página 69 de 93 www.coljuegos.gov.co	 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 y no pagadas. • 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.  Página 70 de 93 www.coljuegos.gov.co



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.

- 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.

- 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



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.

Página 74 de 93

www.coljuegos.gov.co
Página 74 de 93

Página 74 de 93

www.coljuegos.gov.co



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.
direccion_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)	
1	2
3	4
5	6
7	8
9	10
11	12
13	14
15	16
17	18
19	20
21	22
23	24
25	26
27	28
29	30
31	32
33	34
35	36
37	38
39	40
41	42
43	44
45	46
47	48
49	50
51	52
53	54
55	56
57	58
59	60
61	62
63	64
65	66
67	68
69	70
71	72
73	74
75	76
77	78
79	80
81	82
83	84
85	86
87	88
89	90
91	92
93	94
95	96
97	98
99	100

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 (Si 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 ticket y/o boleta electrónica con IVA.





valor_boleta_sin_iva	Valor de venta al público de cada ticket y/o boleto electrónico IVA.
cantidad_boletas	Número de tickets 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, 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.
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
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



INFORMACIÓN DE ENTIDADES TERRITORIALES	
Dato	Lista de Valores
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 Tickets Válidos	Número Tickets Válidos



Derechos de explotación y Gastos de administración.

Ventas Netas (En millones)

Mes	Valor Completo	Valor en Millones
Ene	1000	0.01
Feb	1200	0.01
Mar	900	0.00
Abr	1500	0.01
May	1800	0.01
Jun	1800	0.01

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

Página 88 de 93

www.coljuegos.gov.co

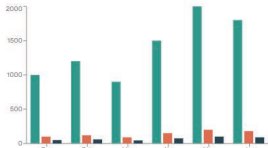




POR PERIODO, PROMEDIO TRIMESTRAL, PROMEDIO MENSUAL y PROMEDIO DÍAS CON SORTEOS.

1. Ventas Netas (En millones)
2. Ajustes, ganadores y premios
3. Derechos de explotación y Gastos de administración

Derechos de Explotación y Gastos de Administración



Periodo	Derechos de Explotación (D.E.)	Gastos de Administración (G.A.)
Ene	1000	100
Feb	1200	100
Mar	900	100
Abr	1500	100
May	2000	200
Jun	1800	200

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.



Página 90 de 93

www.coljuegos.gov.co

