

INFORME DE ANÁLISIS FORENSE SORTEO 09 DE MAYO LOTERÍA DE MEDELLÍN

Preparado para:
Lotería de Medellín
Dr. Rodrigo Alberto Mendoza Vega –
Gerente Lotería de Medellín

Fecha de elaboración:
20 de junio de 2025
Investigador responsable: Leonel Marín
Ramírez

Junio, 2025

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

Tabla de contenido

- 1. Resumen ejecutivo..... 3
 - 1.1. Conclusión principal 3
- 2. Alcance y metodología..... 3
 - 2.1. Alcance 3
 - 2.2. Metodología..... 3
- 3. Entrevistas..... 4
 - 3.1. Personal entrevistado 4
 - 3.2. Hallazgo clave de entrevistas 4
- 4. Observación del sorteo en vivo e inspección física de equipos..... 4
 - 4.1. Acceso al “templo de los millones” 4
 - 4.2. Ejecución del presorteo..... 5
 - 4.3. Ejecución del sorteo..... 5
- 5. Análisis forense de logs..... 6
 - 5.1. Evidencia entregada por el equipo de TI de la Lotería de Medellín 6
 - 5.2. Análisis de logs del servidor de aplicaciones..... 6
 - 5.2.1. Logs system.evt 6
 - 5.2.2. Logs system.evt 7
 - 5.2.3. Logs application.evt..... 7
 - 5.2.4. Logs Microsoft Office Sessions.evt 8
 - 5.3. Análisis de logs del firewall..... 8
- 6. Análisis de posibilidad de fraude..... 9
- 7. Conclusiones..... 10
 - 7.1. Fortalezas identificadas..... 10
 - 7.1.1. Controles físicos robustos 10
 - 7.1.2. Garantías de aleatoriedad 10
 - 7.1.3. Transparencia operativa..... 10
 - 7.1.4. Controles Anti-fraude verificados 11
 - 7.2. Observaciones y áreas de mejora..... 11
 - 7.2.1. Limitaciones en trazabilidad digital..... 11
 - 7.2.2. Infraestructura de TI 11
 - 7.2.3. Análisis de logs de Firewall 12

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

1. Resumen ejecutivo

La presente investigación forense digital fue solicitada por la Gerencia de la Lotería de Medellín, con el fin de verificar la integridad, seguridad y aleatoriedad del sistema de sorteos durante la realización del sorteo del 09 de mayo de 2025 de la Lotería de Medellín, teniendo como referencia la norma NTC 6767 para los juegos de suerte y azar.

Para la realización de dicha investigación forense, se realizó una evaluación que incluyó:

- Entrevistas con personal clave para entender el entorno tecnológico para el desarrollo de los sorteos de la lotería.
- Inspección física de los equipos y sistemas que ejecutan los sorteos.
- Inspección de logs del equipo de seguridad perimetral y servidor de aplicaciones.

1.1. Conclusión principal

El sistema cumple con las buenas prácticas de seguridad y aleatoriedad, con algunas observaciones menores en el aspecto de seguridad de TI que no tienen implicaciones directas sobre la ejecución de los sorteos.

2. Alcance y metodología

2.1. Alcance

- Entendimiento de los procedimientos operativos de sorteos.
- Entendimiento de los controles de seguridad física y lógica.
- Observación directa del presorteo y sorteo en la lotería de Medellín.
- Análisis forense de logs de seguridad perimetral (Fortinet FortiGate).
- Análisis forense de logs del servidor de aplicaciones (Windows Server 2003).

2.2. Metodología

- Entrevistas con personal clave.
- Observación de sorteo en vivo e inspección equipos del sorteo.
- Análisis forense de logs.
- Análisis de posibilidad de fraude.
- Elaboración de informe y recomendaciones.

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

3. Entrevistas

3.1. Personal entrevistado

NOMBRE	CARGO	FECHA
Rodrigo Alberto Mendoza Vega	Gerente	13 de junio de 2025
Julián Mauricio Montoya	Director de TI	13 de junio de 2025
Álvaro Villegas Díaz	Subgerente de Planeación	13 de junio de 2025

3.2. Hallazgo clave de entrevistas

Fortalezas:

- Se tienen un procedimiento claro de asignación de las personas que acompañan los presorteos y sorteos, garantizando que se cuente con la asistencia de las autoridades y entes de control para la supervisión de los presorteos y sorteos.
- Se evidencia una separación lógica y procedimental entre los procesos de TI y la operación de los sorteos.
- El equipo de TI apoya a la Dirección de Loterías en la ejecución del proceso de “Devolución” que implica que antes de las 10:00 pm se envía a la Superintendencia de Salud y a Coljuegos la información de las ventas y los números que participan en el sorteo.

4. Observación del sorteo en vivo e inspección física de equipos

4.1. Acceso al “templo de los millones”

Para el acceso al “templo de los millones” que es el lugar donde se realiza el sorteo, se evidencian los siguientes controles:

- Autorización previa por parte de la empresa para el acceso.
- Registro de ingreso en una minuta por parte del personal de seguridad de la empresa.
- Sólo ingresan todas las personas que van a estar en el sorteo, hasta tanto se encuentren las autoridades invitadas.
- El acceso se hace por parte del personal técnico con acceso, mediante huella y carné de autenticación.

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

- No se permite el ingreso de aparatos celulares.
- El recinto cuenta con 6 cámaras de seguridad que son monitoreadas desde el equipo de TI.
- El recinto cuenta con ventanas que dan a la calle y siempre puede ser visto su interior desde la calle, incluso los sorteos son vistos por personas que se ubican fuera del recinto. Las vidrieras de las ventanas son de seguridad.

4.2. Ejecución del presorteo

Se evidencian las siguientes fortalezas en la ejecución del presorteo:

- Se inicia alrededor de las 8:30 pm.
- Asignación aleatoria y automática de juegos de balotas para los diferentes números del sorteo.
- Cada balotera tiene su propio compresor para impulsar las balotas.
- El presorteo se ejecuta en 10 veces para validar que no hayan balotas que se repitan más de 5 veces en cada balotera y pueda afectar la aleatoriedad del sorteo.
- Las balotas se pesan de manera mensual y de manera automática por los mismos equipos del sorteo.
- El sistema incluye módulos para almacenamiento de las balotas, transporte neumático de balotas, y control central para operar el sorteo.
- Después del presorteo las baloteras y demás equipos quedan listos para el sorteo, para lo cual todos los asistentes salen del “Templo de los millones” y en las puertas se pone un sello hasta que las autoridades y asistentes ingresan nuevamente al momento del sorteo.

4.3. Ejecución del sorteo

Se evidencian las siguientes fortalezas en la ejecución del sorteo:

- Se ejecuta la transmisión en vivo del sorteo del premio mayor a través del canal de televisión Teleantioquia.
- Se ejecuta la transmisión en vivo del sorteo de los premios secos a través de las redes sociales de la lotería.
- Tanto las autoridades, como el personal técnico de la lotería y la máquina que controla la ejecución del sorteo registran los resultados de cada sorteo para realizar el acta al final.

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

5. Análisis forense de logs

5.1. Evidencia entregada por el equipo de TI de la Lotería de Medellín

El equipo de TI de la Lotería entrega en un disco externo los siguientes archivos con la evidencia:

Archivo 727E2B46CA6C1558C46F0BF35ECCB2446FE87668.log

- MD5: 7880aa1e7a76a91c84ba8968a9c67535
- Sha1: 727e2b46ca6c1558c46f0bf35eccb2446fe87668
- Sha256:a883a63cdee4907efdfb7dd6765dbb611221781b3795f324c6c780e452878039

Archivo EBC9D0AA65F32EF5C3117373BBFB2127E2DADC29.zip

- MD5: 7ca3fld7fb3f67589e56869309680461
- Sha1: ebc9d0aa65f32ef5c3117373bbfb2127e2dad29
- Sha256:51e88b4da9379a552630a9dd6714ab2cbfe249c3a41b3b69aa94234f6e3b3450

5.2. Análisis de logs del servidor de aplicaciones

Logs proporcionados:

NOMBRE	DESDE	HASTA	TAMAÑO
System.evt	21/02/2025 1:03:23 pm	30/05/2025 10:23:51 am	16.384 KB
Security.evt	Archivo no permite abrir		53.258 KB
Microsoft Office Sessions.evt	24/11/2011 5:06:44 pm	30/05/2025 10:02:11 am	15.637 KB
Application.evt	28/02/2025 3:15:53 am	30/05/2025 10:23:09 am	11.126

5.2.1. Logs system.evt

Los eventos registrados el 09 de mayo de 2025 fueron los siguientes:

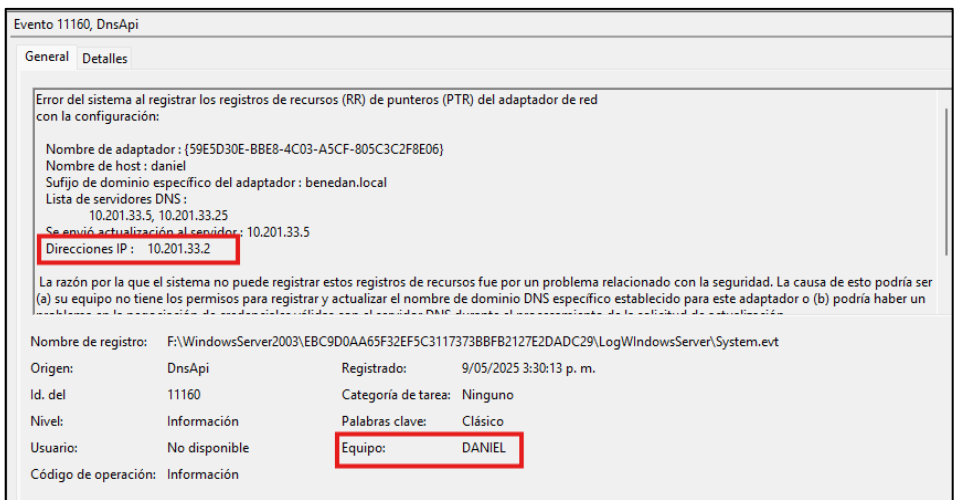
- Advertencia: 19 registros
- Error: 273
- Información: 100

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

Así mismo están clasificados en el siguiente origen:

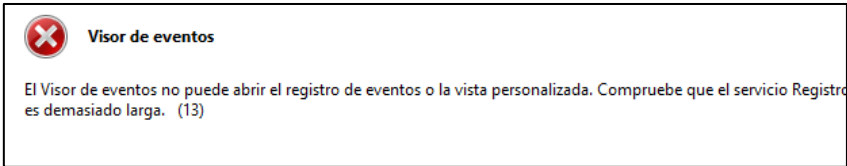
- DnsApi: 01
- EventLog: 01
- Print: 108
- TermServDevices: 273
- W32Time: 09

Ninguno de los eventos es relevante en temas de ciberseguridad, sin embargo, el log DnsApi muestra el nombre del equipo y la IP del servidor:



5.2.2. Logs system.evt

No es posible abrir el archivo, lo que no permite identificar los eventos de seguridad presentados en el servidor para el día del sorteo objeto de análisis.



5.2.3. Logs application.evt

Los eventos registrados el 09 de mayo de 2025 fueron los siguientes:

- Advertencia: 301
- Información: 16

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

Estos están clasificados principalmente en:

- Evento 4098 (group Policy Shortcuts y Group Policy Drive Maps): 286
- Evento Userenv: 26

Ninguno de los anteriores eventos es relevante en temas de ciberseguridad.

5.2.4. Logs Microsoft Office Sessions.evt

No se encuentran eventos relevantes en temas de ciberseguridad.

5.3. Análisis de logs del firewall

A continuación, se muestra un resumen general del archivo de log analizado:

- Total de eventos: 57.334
- Eventos denegados: 11.245
- IPs origen únicas: 7493
- IPs destino únicas: 228
- Registros desde: 10/05/2025 23:46:36
- Registros hasta: 10/05/2025 23:59:59

Los registros no son relevantes para el objeto de la investigación forense relacionada con el sorteo del 09 de mayo de 2025, además que corresponde a una ventana de tiempo de solo 13 minutos y 20 segundos.

No obstante lo anterior, desde el punto de vista de ciberseguridad, es importante considerar lo siguiente:

Se evidencia bloqueo de tráfico SNMP desde la IP 10.201.33.2 que corresponde al servidor de aplicaciones a las IP 150.1.1.200 y 150.1.1.169 que están ubicadas en Japón, lo cual es una anomalía que debería investigarse ya que no es normal.

Se evidencia al menos 13.000 conexiones desde diferentes IPs de Brazil hacia la IP pública de la Lotería de Medellín 190.90.53.67, con el siguiente comportamiento:

- El 95.2% de estas conexiones tienen timeouts, lo cual puede indicar un ataque de denegación de servicio que podría causar una indisponibilidad.
- Ejemplo de algunas IPs de Brasil con reportes negativos de ciberseguridad:

<https://www.abuseipdb.com/check/186.211.99.116>

<https://www.abuseipdb.com/check/186.211.99.19>

<https://www.abuseipdb.com/check/186.211.99.243>

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

<https://www.abuseipdb.com/check/186.211.99.116>

<https://www.abuseipdb.com/check/186.211.99.33>

<https://www.abuseipdb.com/check/186.211.99.33>

<https://www.abuseipdb.com/check/168.205.33.74>

6. Análisis de posibilidad de fraude

Para hacer este análisis de posibilidad de fraude con las máquinas baloteras utilizadas por la Lotería de Medellín para los sorteos, se toma como referencia un estudio detallado emplea un sistema Bayesiano para analizar el comportamiento aleatorio en juegos de lotería, tomando como base sorteos realizados con baloteras que extraen números de una urna transparente mediante un sistema de aire que lanza las balotas, que utiliza los mismos principios de la Lotería de Medellín.

El estudio se encuentra publicado en el sitio:

https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100019.

Este trabajo concluye que, aunque el sistema es completamente aleatorio e impredecible, es posible identificar ciertas tendencias en los resultados mediante un clasificador Bayesiano, que permite establecer probabilidades relativas de que ciertos números sean ganadores. Sin embargo, no se puede afirmar con certeza absoluta la predicción de números ganadores.

Conclusión práctica.

El método bayesiano puede identificar tendencias estadísticas, pero:

- NO puede predecir resultados específicos.
- La ventaja obtenida es mínima y no garantiza ganancias.
- Las loterías están diseñadas específicamente para ser impredecibles.

En resumen: Aunque el estudio es académicamente interesante para analizar sistemas aleatorios, no proporciona una forma práctica o confiable de predecir números ganadores de lotería. La probabilidad de ganar sigue siendo la misma que jugando al azar.

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

7. Conclusiones

- No se evidencian anomalías en los procesos que se tienen establecidos para el desarrollo del sorteo.
- La ejecución del proceso, en su gran mayoría de forma automática y con mínima intervención manual, minimiza la posibilidad de errores.
- El mecanismo utilizado en las máquinas que ejecutan el sorteo, especialmente con las baloteras con sistema neumático, ha sido estudiado por su aleatoriedad.
- Se evidencia en las diferentes entrevistas que la infraestructura de TI de la empresa es independiente y no tiene injerencia en los equipos utilizados en el desarrollo del sorteo.

7.1. Fortalezas identificadas

7.1.1. Controles físicos robustos

- Acceso multicapa: Autorización previa + registro + biometría + carné de identificación.
- Monitoreo integral: 6 cámaras de seguridad con supervisión continua desde TI.
- Transparencia física: Ventanas de seguridad con visibilidad pública del proceso.
- Custodia efectiva: Sellado del recinto entre presorteo y sorteo.

7.1.2. Garantías de aleatoriedad

- Sistema neumático independiente: Cada balotera con compresor propio.
- Validación múltiple: Presorteo ejecutado 10 veces para detectar balotas repetitivas (>5 repeticiones).
- Mantenimiento preventivo: Pesaje mensual automático de balotas.
- Asignación automática: Selección aleatoria de juegos de balotas sin intervención manual.

7.1.3. Transparencia operativa

- Presencia de autoridades: Las autoridades y funcionarios de la lotería participan en el proceso.
- Transmisión pública: Sorteo mayor en vivo por Teleantioquia, premios secos por redes sociales.

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

- Separación de funciones: Personal de TI independiente de la operación de sorteos.
- Proceso de "Devolución": Envío de información de ventas y números participantes antes de las 10:00 pm a la Superintendencia de Salud y Coljuegos.

7.1.4. Controles Anti-fraude verificados

- Separación física y temporal entre personal de TI y operación del sorteo.
- Validación múltiple en presorteo para detectar anomalías.
- Presencia de múltiples autoridades durante todo el proceso.
- Transmisión en tiempo real imposibilita manipulación posterior.
- Adicionalmente y teniendo como base el estudio referenciado, se puede concluir que:
 - Los sistemas de baloteras neumáticas son inherentemente aleatorios e impredecibles.
 - No existe método práctico para predecir resultados específicos.
 - Las tendencias estadísticas identificables no proporcionan ventaja significativa para manipulación.
 - La probabilidad de ganar permanece idéntica al juego completamente aleatorio.

7.2. Observaciones y áreas de mejora

7.2.1. Limitaciones en trazabilidad digital

- Logs de seguridad inaccesibles: Archivo Security.evt (53.258 KB) no permite apertura.
- Ventana temporal limitada: Logs de firewall disponibles solo por 13 minutos del 10/05/2025, los cuales no corresponden al día del sorteo a analizar.

7.2.2. Infraestructura de TI

- Sistema operativo discontinuado: Windows Server 2003 sin soporte de seguridad desde 2015.
- Eventos del sistema: No se están obteniendo logs relevantes en materia de ciberseguridad.
- Conexiones anómalas: Tráfico SNMP desde servidor principal hacia IPs en Japón.

Código	Fecha	Versión	Tipo	Cliente
LM-01	20/06/2025	2.0	CONFIDENCIAL	L.MEDELLÍN

7.2.3. Análisis de logs de Firewall

- Actividad de red: 57.334 eventos totales, 11.245 denegados.
- Conexiones externas: Mas de 13.000 conexiones desde Brasil, de las cuales el 95.2% son Timeouts que pueden indicar un ciberataque y que no está siendo bloqueado por el firewall.

Cordialmente,

LEONEL MARIN RAMÍREZ

Ingeniero Informático

Matrícula Profesional No 05833-170300