

|                          |                                                                                         |
|--------------------------|-----------------------------------------------------------------------------------------|
| Alerta ID:               | 132                                                                                     |
| Fecha del reporte:       | 12/08/2026                                                                              |
| Entidad:                 | Todas las Entidades del Ecosistema Digital                                              |
| Título:                  | eventos de tráfico permitido desde direcciones IP clasificadas en listas negras (IPSum) |
| Herramienta de detección | FortiSIEM                                                                               |
| Activo involucrado:      | Infraestructura tecnológica y servicios de red de entidades públicas                    |
| Tipo de alerta:          | Boletín informativo                                                                     |
| Nivel de riesgo:         | Alto                                                                                    |

### Resumen ejecutivo



El CSIRT Salud identificó, mediante la plataforma SIEM sectorial, 95.912 eventos de tráfico entrante procedentes de 200 direcciones IP únicas clasificadas en la lista negra IPSum (malware / botnet),

La criticidad del hallazgo se mantiene alta. En el 100 % de los registros el campo de acción del firewall no se encuentra poblado, por lo que no es posible confirmar desde el SIEM si el tráfico fue permitido o denegado; cada entidad debe verificar el estado efectivo del bloqueo en su perímetro. Adicionalmente, el volumen presenta una tendencia creciente durante el período, pasando de 13.600 eventos en la semana del 1 de julio a 30.464 en la semana del 27 de julio.

### Descripción del Incidente



**Fuente de detección:** SIEM sectorial.

**Categoría:** Tráfico permitido desde IPs maliciosas (IPSum).



**Severidad:** Alta.

**Volumen:** 95.912 eventos, 200 direcciones IP de origen únicas, 32 activos de destino y 5 entidades con registros.

**Patrón identificado:** conexiones desde rangos asociados a **malware, botnets y servidores de comando y control (C2)**.

**Patrón identificado:** conexiones originadas mayoritariamente en proveedores de hosting y servidores virtuales (DigitalOcean, RouterHosting/Cloudzy, OVH y similares), cuyos rangos son reportados de forma recurrente por escaneo de puertos, intentos de autenticación por fuerza bruta y distribución de malware.

**Comportamiento observado:** persistencia en intentos de conexión desde múltiples geolocalizaciones (Estados Unidos, Francia, Holanda, Canada, entre otros).

A continuación, se relaciona el Top las direcciones IP identificadas durante el análisis en el SIEM. Estos registros corresponden a eventos de tráfico permitido desde orígenes clasificados como maliciosos en listas negras (IPSum). La información se presenta de manera consolidada para servir como referencia en la gestión de riesgos y la implementación de medidas de mitigación.

### Clasificación de los indicadores

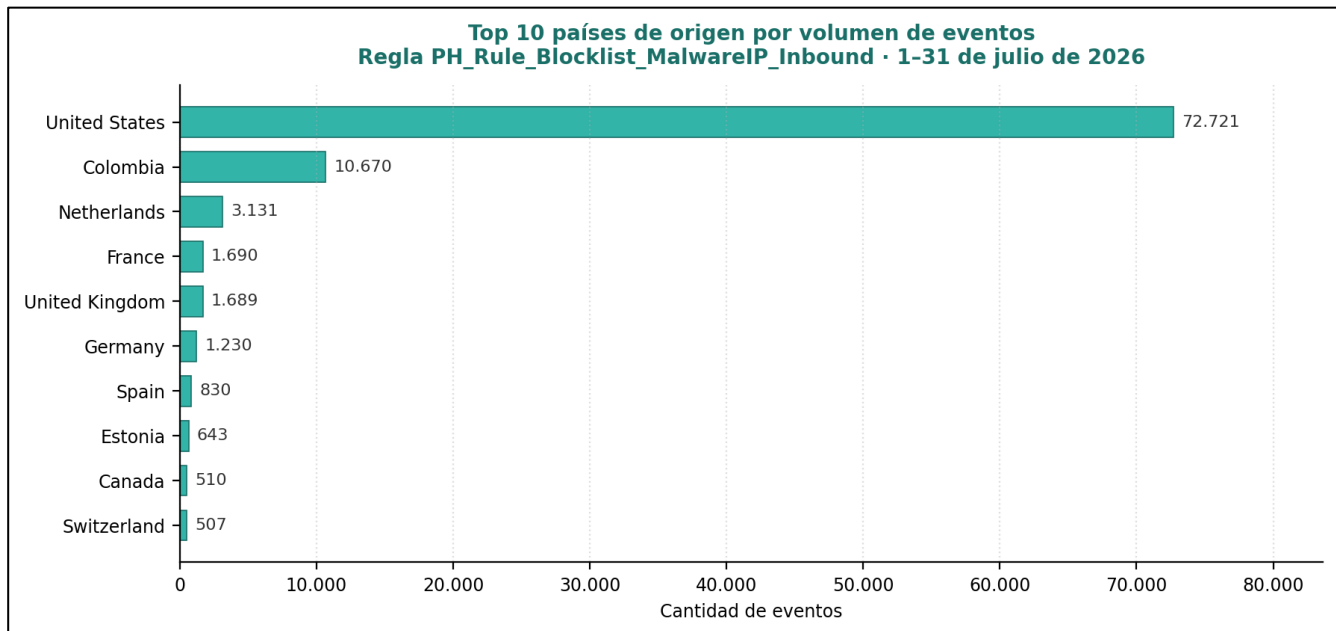


El CSIRT Salud contrastó las 200 direcciones IP contra los rangos oficiales publicados por los operadores de servicios legítimos de Internet y contra fuentes de reputación. El resultado se presenta a continuación:

| Clasificación             | IP  | Eventos | % eventos | Sustento                                                                                                                                                                          |
|---------------------------|-----|---------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bloqueo / investigación   | 154 | 59.119  | 61,6 %    | Infraestructura de hosting, VPS y direcciones residenciales sin atribución legítima. Requieren bloqueo y verificación en el perímetro.                                            |
| Escaneo de reconocimiento | 7   | 27.083  | 28,2 %    | Rango 207.90.244.0/24, registrado a nombre de Shodan LLC (motor de búsqueda de dispositivos expuestos). No constituye malware, pero evidencia exposición de servicios publicados. |
| Falso positivo probable   | 39  | 9.710   | 10,1 %    | Rastreadores de motores de búsqueda: Googlebot (66.249.64.0/19), Bingbot (40.77.167.0/24, 207.46.13.0/24, 52.167.144.0/24, 157.55.39.0/24) y DotBot/Moz (216.244.66.0/24).        |



**Recomendación asociada:** las 39 direcciones clasificadas como falso positivo probable **no deben bloquearse** sin validación previa, ya que su bloqueo puede afectar la indexación de los portales institucionales. Se recomienda confirmar cada dirección mediante resolución DNS inversa (debe resolver al dominio googlebot.com, search.msn.com o al dominio del operador correspondiente) antes de excluirla y notificar el resultado al CSIRT Salud para depurar la regla de correlación.



Estados Unidos concentra 72.721 eventos (75,8 %) originados en 89 direcciones IP, en su mayoría asociadas a proveedores de infraestructura en la nube. **Colombia es el segundo origen, con 58 direcciones IP y 10.670 eventos (11,1 %)**, dirigidos principalmente a ADRES. Este último dato merece atención particular: se trata de direcciones nacionales, presumiblemente asignadas a usuarios o equipos comprometidos dentro del país, que podrían corresponder a accesos legítimos de usuarios cuya dirección quedó incluida en la lista negra, o a equipos infectados dentro de redes de proveedores locales. Su bloqueo indiscriminado podría afectar el acceso de usuarios legítimos a los servicios de la entidad, por lo que se recomienda su validación individual.

## Principales indicadores identificados

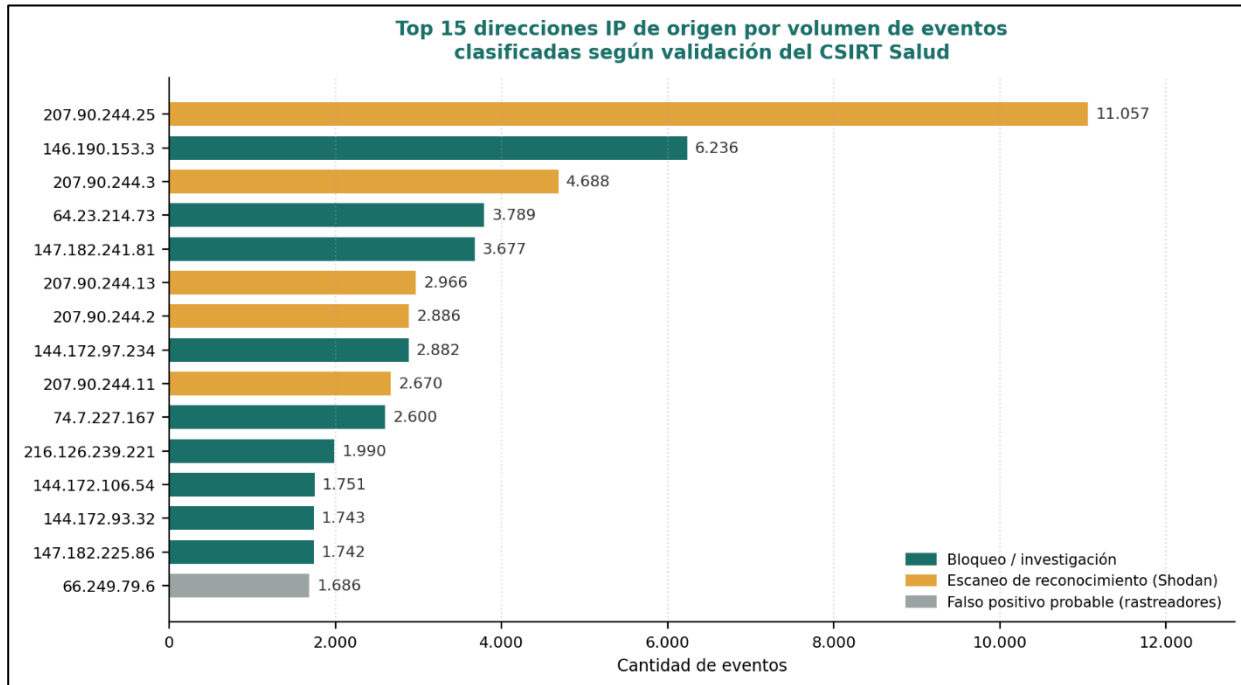


Figura 3. Top 15 de direcciones IP de origen por volumen de eventos, según clasificación.

## Bloques de red con actividad concentrada



Se identificaron bloques de red desde los cuales opera más de una dirección IP contra los mismos activos. En estos casos el bloqueo por bloque completo (CIDR /24) resulta más eficaz que el bloqueo individual, dado que el atacante rota direcciones dentro del mismo rango:

| Bloque de red    | IP | Eventos | País           |
|------------------|----|---------|----------------|
| 172.110.223.0/24 | 3  | 1.242   | United States  |
| 45.205.1.0/24    | 9  | 1.000   | United States  |
| 160.119.71.0/24  | 2  | 457     | United Kingdom |
| 143.105.99.0/24  | 3  | 446     | Colombia       |



| Bloque de red    | IP | Eventos | País                      |
|------------------|----|---------|---------------------------|
| 181.48.176.0/24  | 2  | 396     | Colombia                  |
| 185.178.231.0/24 | 2  | 395     | Spain                     |
| 185.243.5.0/24   | 2  | 382     | Hong Kong / United States |
| 94.154.43.0/24   | 3  | 376     | United Kingdom            |
| 195.178.110.0/24 | 2  | 336     | Netherlands               |
| 45.194.67.0/24   | 2  | 240     | Dominican Republic        |

### Impacto potencial



- **Reconocimiento y descubrimiento** de servicios, versiones y puertos expuestos, como etapa previa a un intento de explotación.
- **Intentos de acceso no autorizado** mediante fuerza bruta o explotación de vulnerabilidades en los servicios publicados.
- **Descarga o propagación de malware** en equipos internos, en caso de que exista un canal de comunicación establecido.
- **Compromiso de información sensible** alojada en los sistemas expuestos.
- **Ataques de denegación de servicio (DDoS)** contra los servicios publicados de la entidad.
- **Afectación reputacional y operativa** en caso de explotación exitosa.

### Recomendaciones



- **Verificar la acción del perímetro.** Confirmar en los registros del firewall si el tráfico asociado a estas direcciones fue permitido o denegado, dado que el SIEM no reporta este campo. Es la primera acción a ejecutar.



- **Bloquear las 154 direcciones IP** clasificadas para bloqueo en firewalls y controles de red, priorizando el bloqueo por bloque completo (CIDR /24) en los rangos relacionados en este boletín.
- **No bloquear las 39 direcciones clasificadas como falso positivo probable** sin validación previa mediante DNS inverso, e informar el resultado al CSIRT Salud.
- **Atender la exposición evidenciada por el escaneo de reconocimiento.** Inventariar los servicios publicados a Internet, deshabilitar los que no sean requeridos, ocultar banners y versiones de software, y verificar que los servicios expuestos cuenten con parches al día.
- **Configurar las direcciones como loC** en las herramientas de seguridad (EDR, firewall, proxy) para activar alertas y cortar la comunicación.
- **Revisar los registros históricos** de los activos de destino con mayor volumen de eventos, con el fin de descartar accesos exitosos o movimiento lateral posterior.
- **Fortalecer las políticas de filtrado perimetral**, de forma que este tipo de tráfico no sea permitido sin análisis previo, y evaluar la aplicación de restricciones geográficas donde el servicio lo permita.
- **Mantener monitoreo constante** en busca de patrones similares, considerando la tendencia creciente observada durante el período.

## Conclusión



El hallazgo evidencia actividad automatizada y sostenida desde direcciones incluidas en listas negras hacia infraestructura publicada del sector salud, con una tendencia creciente durante el mes de julio de 2026. El ejercicio de validación permitió depurar el 38,3 % del volumen de eventos, atribuible a rastreadores legítimos y a motores de búsqueda de dispositivos expuestos, y focalizar la acción sobre 154 indicadores que requieren bloqueo efectivo. Es fundamental que cada entidad confirme el estado del bloqueo en su perímetro, atienda la

exposición de servicios evidenciada y fortalezca la supervisión de eventos en el SIEM, a fin de reducir el riesgo de intrusión y compromiso de sistemas críticos.

En caso de que, después de verificar las direcciones IP reportadas, se detecte que algunas corresponden a direcciones permitidas o a servicios legítimos de la entidad, por favor reportarlas al correo electrónico del CSIRT Salud con el fin de que estas sean excluidas y así evitar que sean reportadas nuevamente por el SIEM.

### Fuentes



- Herramienta de monitoreo FortiSIEM — CSIRT Salud.
- IPsum — lista de direcciones IP maliciosas agregada (<https://github.com/stamparm/ipsum>).
- Google — rangos oficiales de Googlebot (<https://developers.google.com/search/apis/ipranges/googlebot.json>).
- Microsoft Bing — rangos oficiales de Bingbot (<https://www.bing.com/toolbox/bingbot.json>).
- <https://www.virustotal.com/gui/home/upload>
- <https://www.abuseipdb.com/>
- Registro regional de Internet ARIN — consulta WHOIS de bloques de red.

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico [contacto@csirtsalud.gov.co](mailto:contacto@csirtsalud.gov.co). Nuestro equipo está disponible para brindar el acompañamiento necesario.

