

Alerta ID:	02
Fecha del reporte:	17/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Posibles ciberataques contra infraestructuras críticas y entidades del Estado con ocasión de la conmemoración del 20 de julio
Herramienta de detección	N/A
Activos involucrados:	infraestructuras críticas y portales institucionales
Tipo de alerta:	Informativa
Nivel de riesgo:	Alto

Objetivo:

Con ocasión de la conmemoración del Día de la Independencia Nacional, el próximo 20 de julio de 2026, el CSIRT Salud advierte sobre el incremento en la probabilidad de materialización de ciberataques dirigidos contra infraestructuras críticas y portales institucionales de entidades del Estado colombiano, incluidas las entidades del sector salud. Las fechas conmemorativas de relevancia nacional han sido históricamente aprovechadas por colectivos hacktivistas y actores de amenaza oportunistas para ejecutar campañas de denegación de servicio, desfiguración de sitios web (defacement), suplantación de identidad institucional y phishing temático, con el propósito de obtener visibilidad mediática, afectar la disponibilidad de servicios ciudadanos o comprometer información institucional.

El presente boletín tiene carácter preventivo. Su objetivo es que las entidades de la comunidad CSIRT Salud fortalezcan de manera anticipada su postura defensiva durante el periodo comprendido entre el 17 y el 21 de julio de 2026, y conozcan, a título de referencia de buenas prácticas, el conjunto de acciones de endurecimiento implementadas por el Ministerio de Salud y Protección Social ante este escenario de amenaza.

Descripción:

Existen antecedentes documentados de actividad maliciosa dirigida contra entidades estatales colombianas en coyunturas conmemorativas y de alta sensibilidad social. El 20 de julio de 2011, en el marco de la denominada operación #OpIndependencia, colectivos hacktivistas dejaron fuera de servicio el portal del Ministerio de Defensa Nacional durante aproximadamente doce horas consecutivas, afectaron el sitio de la Alta Consejería para el Bicentenario y comprometieron cuentas oficiales en redes sociales de altos funcionarios del Estado. Posteriormente, durante el Paro Nacional de 2021, la operación #OpColombia ocasionó la indisponibilidad de múltiples portales gubernamentales y la exposición de información de las fuerzas armadas.

Adicionalmente, el sector salud ha sido impactado de manera directa por incidentes de gran escala: el ataque de ransomware contra el proveedor IFX Networks en septiembre de 2023 afectó a más de setenta entidades públicas, entre ellas el Ministerio de Salud y Protección Social y la Superintendencia Nacional de Salud, comprometiendo la disponibilidad de servicios de atención al ciudadano.

El panorama de 2026 agrava este escenario. Los informes oficiales de ciberseguridad proyectan para el presente año la intensificación de ataques dirigidos contra infraestructura crítica mediante el uso de phishing avanzado apoyado en inteligencia artificial generativa, suplantaciones mediante deepfakes, técnicas de evasión de autenticación multifactor (MFA) y automatización del reconocimiento de sistemas vulnerables, señalando de manera explícita al sector salud y a las entidades de gobierno entre los sectores de mayor exposición. El contexto electoral del año 2026 constituye un factor adicional de motivación para colectivos hacktivistas con agendas políticas, lo que incrementa la probabilidad de operaciones coordinadas alrededor de fechas simbólicas como el 20 de julio.

Vectores de ataque esperados



Con base en los antecedentes descritos y en el comportamiento observado de los actores de amenaza que operan en la región, se identifican como más probables los siguientes vectores durante el periodo de vigilancia:

- **Ataques de denegación de servicio distribuida (DDoS)** contra portales web institucionales y servicios ciudadanos expuestos a Internet, orientados a afectar la disponibilidad en la fecha conmemorativa.
- **Desfiguración (defacement)** de sitios web con mensajes de contenido político o reivindicativo, buscando visibilidad mediática.
- **Campañas de phishing temático** con asuntos alusivos a la conmemoración, comunicados institucionales falsos, supuestas jornadas o beneficios, distribuidas por correo electrónico y mensajería (smishing).
- **Suplantación (spoofing)** de dominios y perfiles institucionales en redes sociales, para difundir desinformación o recolectar credenciales de funcionarios y ciudadanos.
- **Explotación de servicios** expuestos a Internet (VPN, portales de autenticación, aplicaciones web con vulnerabilidades conocidas), aprovechando la reducción de personal operativo durante el fin de semana festivo.
- **Uso de credenciales comprometidas** obtenidas mediante malware de tipo stealer o filtraciones previas, como vector de acceso inicial para intrusiones y despliegue de ransomware oportunista.

Acciones preventivas para tomar



Ante el escenario descrito, se presenta a continuación un conjunto de acciones e ítems de endurecimiento preventivo sobre la infraestructura tecnológica, a tener en cuenta para mejorar la postura de ciberseguridad ante la conmemoración del 20 de julio. Se comparten con la

comunidad CSIRT Salud como referencia de buenas prácticas, para que cada entidad evalúe su adopción de acuerdo con sus capacidades y arquitectura de seguridad.

Protección de punto final (endpoint)

- **Elevar el nivel de detección a "Alto"** en las herramientas de protección de endpoint, permitiendo identificar comportamientos anómalos o sofisticados en los dispositivos.
- **Tener en cuenta que esta configuración incrementa la sensibilidad**, por lo que puede generar un aumento de falsos positivos, situación que deberá gestionarse con los equipos de soporte.
- **Actualizar los motores de análisis** y reforzar el monitoreo basado en comportamiento y en firmas emergentes.

Antispam y filtros perimetrales de correo

- **Fortalecer los filtros antispam** y de análisis de contenido en los sistemas de correo corporativo.
- **Activar reglas avanzadas** para la detección de enlaces dinámicos, ofuscados y patrones comunes en ataques de tipo phishing.
- **Ajustar las reglas de clasificación** para reforzar la prevención de entrega de mensajes maliciosos en las bandejas de entrada.

Proxies y filtrado de navegación web

- **Endurecer las políticas de navegación** en los proxies corporativos.
- **Bloquear los accesos** a dominios recientemente creados o sin reputación comprobada.
- **Activar el bloqueo por geolocalización**, denegando conexiones hacia y desde regiones de alto riesgo.

Dispositivos de seguridad perimetral

- **Implementar controles más estrictos** en firewalls y gateways de seguridad.
- **Elevar la sensibilidad** de los motores de detección de amenazas a niveles altos.

- **Reforzar las conexiones entrantes y salientes** con políticas más estrictas, incluyendo filtrado por geolocalización y ajuste de listas de control de acceso (ACL).

Soluciones avanzadas de detección y respuesta extendida (XDR)

- **Implementar reglas avanzadas** de detección de amenazas persistentes en las plataformas de detección y respuesta extendida.
- **Activar políticas de análisis profundo** para la correlación de eventos y la identificación de comportamiento sospechoso a nivel de red y de endpoint.

Sensibilización a usuarios y gestión de equipos no corporativos

- **Generar y divulgar piezas** de materiales de sensibilización dirigidos a los usuarios, con el apoyo de las áreas de seguridad de la información.
- **Instar a funcionarios y contratistas a mantenerse alerta** ante intentos de suplantación o engaño a través del correo electrónico u otros medios, especialmente durante el periodo conmemorativo.
- **Considerar como factor de riesgo el uso de equipos personales**, especialmente por parte de contratistas, dado que estos dispositivos no siempre cuentan con las políticas y herramientas corporativas de protección; se sugiere adoptar medidas adicionales para mitigar este riesgo.

Recomendaciones para las entidades.

El CSIRT Salud recomienda a las entidades de la comunidad adoptar, en la medida de sus capacidades, las siguientes acciones durante el periodo de vigilancia reforzada:

- **Implementar las medidas de endurecimiento temporal** descritas sobre sus plataformas de protección de endpoint, correo, navegación, perímetro y detección y respuesta, evaluando el impacto operativo del incremento de sensibilidad.

- **Reforzar el monitoreo de disponibilidad** de los portales web institucionales y servicios expuestos a Internet, verificando la capacidad de mitigación de ataques de denegación de servicio con los proveedores correspondientes.
- **Verificar la existencia y validez de copias de seguridad** recientes de los sistemas de información críticos, incluyendo pruebas de restauración, y confirmar que existan copias fuera de línea o inmutables.
- **Confirmar la aplicación de autenticación multifactor (MFA)** en todos los accesos remotos y cuentas privilegiadas, y revisar la vigencia de las credenciales de administración.
- **Fortalecer los turnos de monitoreo** durante el puente festivo, asegurando la disponibilidad de personal de guardia y la actualización de los árboles de llamado y procedimientos de escalamiento.
- **Activar las alertas tempranas** internas ante cualquier indicio de suplantación de dominios, perfiles falsos en redes sociales o campañas de phishing que utilicen la imagen institucional.
- **Reportar cualquier evento o incidente de seguridad** de manera inmediata al CSIRT Salud, a través de los canales institucionales establecidos, para su análisis, correlación sectorial y apoyo en la contención.

Referencias

- Ingeniería Crítica (2011). Comunicado conjunto de Anonymous Colombia acerca de la #OpIndependencia.
- WeLiveSecurity – ESET (2011). Anonymous ataca cuentas oficiales del Gobierno de Colombia en el marco del 20 de julio.
- Semana (2023). Ciberataque a IFX Networks: afectación a entidades del Gobierno colombiano, incluidos Minsalud y Supersalud.
- MinTIC (2026). Informe de ciberseguridad: balance 2025 y proyecciones 2026 para infraestructura crítica.

- Electroners (2025). Hacktivismo: la amenaza digital que pone en jaque a empresas e instituciones en Colombia.

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) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.