

Alerta ID:	03
Fecha del reporte:	22/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Recomendaciones para el fortalecimiento de la postura de ciberseguridad del sector salud frente al incremento de ataques contra entidades públicas colombianas
Herramienta de detección	N/A
Activos involucrados:	Infraestructura tecnológica, servicios expuestos a Internet, identidades digitales, plataformas de colaboración, servicios en la nube, sistemas de información institucional, Historia Clínica Electrónica (HCE), sistemas administrativos, plataformas de atención al ciudadano, dispositivos médicos conectados (IoMT), redes corporativas, infraestructura de respaldo, centros de datos y demás activos críticos del sector salud.
Tipo de alerta:	Informativa
Nivel de riesgo:	Alto

Objetivo:

Durante los últimos meses se ha evidenciado un incremento en la actividad de actores de amenaza dirigidos contra entidades públicas colombianas e infraestructuras críticas, mediante campañas de phishing altamente dirigidas, explotación de vulnerabilidades conocidas, compromiso de identidades digitales, acceso no autorizado a servicios en la nube, exfiltración de información y esquemas de doble extorsión asociados con ataques de ransomware. Estos incidentes demuestran la necesidad de fortalecer las capacidades de prevención, detección, respuesta y recuperación frente a amenazas cibernéticas que puedan afectar la continuidad de los servicios esenciales del Estado.

Aunque los ataques recientes no se han concentrado exclusivamente en el sector salud, las tácticas, técnicas y procedimientos (TTP) empleados por los actores de amenaza pueden ser utilizados contra hospitales, clínicas, Empresas Promotoras de Salud (EPS), Instituciones Prestadoras de Servicios de Salud (IPS), Empresas Sociales del Estado (ESE), Secretarías de Salud y demás organizaciones que administran información clínica y soportan procesos críticos para la atención de la población.

El presente boletín tiene como propósito divulgar recomendaciones técnicas y organizacionales orientadas a fortalecer la postura de ciberseguridad de las entidades del sector salud colombiano, promoviendo la implementación de controles que permitan reducir la superficie de ataque, proteger los activos críticos, fortalecer la resiliencia institucional y mejorar la capacidad para prevenir, detectar, responder y recuperarse frente a incidentes de seguridad de la información.

Descripción:

Durante los últimos años, las amenazas cibernéticas dirigidas contra entidades públicas e infraestructuras críticas han evolucionado hacia operaciones cada vez más sofisticadas, persistentes y orientadas al compromiso de información sensible. Los actores de amenaza han pasado de ejecutar ataques oportunistas a desarrollar campañas dirigidas que combinan ingeniería social, explotación de vulnerabilidades, compromiso de credenciales, acceso indebido a servicios en la nube y exfiltración de información como mecanismo de presión y extorsión.

En Colombia, los incidentes registrados recientemente en entidades públicas y organizaciones estratégicas, incluido el incidente reportado por Ecopetrol, evidencian que las organizaciones continúan siendo objetivo de ataques que buscan comprometer simultáneamente la confidencialidad, integridad y disponibilidad de la información. Estas campañas demuestran que ningún sector se encuentra exento de este riesgo y que los atacantes continúan adaptando sus técnicas para incrementar la probabilidad de éxito.

El sector salud representa un objetivo de especial interés debido al alto valor de la información clínica que administra, la creciente adopción de tecnologías digitales, el uso de plataformas de Historia Clínica Electrónica, servicios en la nube, dispositivos médicos conectados y sistemas que soportan la prestación de servicios esenciales. En este contexto, resulta indispensable fortalecer continuamente los controles de ciberseguridad y adoptar medidas preventivas que permitan reducir la probabilidad de materialización de incidentes y minimizar su impacto sobre la prestación de los servicios de salud.

Principales vectores de ataque observados



Con base en los incidentes registrados recientemente en entidades públicas colombianas, en la información compartida por organismos nacionales e internacionales de ciberseguridad y en las tendencias observadas durante los procesos de respuesta a incidentes, el CSIRT Salud identifica los siguientes vectores de ataque como los de mayor probabilidad de afectar a las entidades del sector salud:

- **Phishing y Spear Phishing:** campañas dirigidas mediante correo electrónico, mensajería instantánea o llamadas fraudulentas para obtener credenciales, distribuir malware o inducir la ejecución de archivos maliciosos.
- **Compromiso de credenciales e identidades digitales:** utilización de credenciales obtenidas mediante filtraciones, robo de información, ataques de fuerza bruta o reutilización de contraseñas para acceder a plataformas institucionales y servicios en la nube.
- **Explotación de vulnerabilidades conocidas:** aprovechamiento de fallas de seguridad en sistemas operativos, aplicaciones, dispositivos de seguridad perimetral, VPN, servicios expuestos a Internet y plataformas de virtualización que no han sido actualizadas oportunamente.
- **Compromiso de servicios en la nube:** acceso no autorizado a plataformas SaaS, IaaS y PaaS mediante configuraciones inseguras, permisos excesivos, autenticación multifactor deshabilitada o aplicaciones de terceros con privilegios elevados.
- **Ransomware y doble extorsión:** campañas que combinan el robo de información con el cifrado de sistemas para exigir pagos económicos bajo la amenaza de divulgar públicamente la información comprometida.
- **Ataques a la cadena de suministro:** compromiso de proveedores tecnológicos, servicios administrados, aplicaciones de terceros o componentes de software utilizados por las organizaciones para facilitar el acceso a múltiples entidades a través de un único punto de entrada.

Recomendaciones para el fortalecimiento de la postura de ciberseguridad

Protección de identidades digitales

Las identidades digitales constituyen actualmente el principal objetivo de los actores de amenaza debido a que el compromiso de una cuenta legítima puede facilitar el acceso a múltiples servicios institucionales sin necesidad de explotar vulnerabilidades adicionales. Los incidentes recientes evidencian que gran parte de las intrusiones exitosas tienen su origen en el uso de credenciales comprometidas, autenticaciones débiles o privilegios excesivos. En consecuencia, las entidades del sector salud deben fortalecer la administración de identidades, privilegiando el principio de mínimo privilegio y la autenticación robusta para todos los usuarios, especialmente aquellos con funciones administrativas.

El CSIRT Salud recomienda implementar las siguientes medidas:

- Habilitar autenticación multifactor (MFA) para todos los accesos remotos, cuentas administrativas, servicios en la nube y aplicaciones críticas.
- Revisar periódicamente las cuentas privilegiadas para verificar que únicamente mantengan los permisos estrictamente necesarios para el desempeño de sus funciones.
- Eliminar o deshabilitar de manera oportuna las cuentas de usuarios retirados, contratistas, proveedores y cuentas temporales que ya no sean requeridas.
- Implementar políticas robustas de contraseñas que contemplen longitud mínima, complejidad adecuada, protección frente a contraseñas comprometidas y restricción del uso de credenciales reutilizadas.
- Restringir el uso de cuentas administrativas para actividades cotidianas como navegación web, correo electrónico o consulta documental.
- Revisar periódicamente los registros de autenticación para identificar intentos reiterados de acceso, autenticaciones desde ubicaciones inusuales, accesos simultáneos desde diferentes ubicaciones geográficas y demás comportamientos anómalos.
- Implementar procesos periódicos de recertificación de privilegios para garantizar que los permisos asignados continúen siendo acordes con las responsabilidades de cada usuario.

Protección del correo electrónico

El correo electrónico continúa siendo uno de los principales vectores utilizados para obtener acceso inicial a las organizaciones mediante campañas de phishing, distribución de malware y robo de credenciales. La incorporación de herramientas basadas en inteligencia artificial ha incrementado considerablemente la calidad de los mensajes fraudulentos, dificultando su identificación por parte de los usuarios. En este contexto, resulta indispensable fortalecer los controles técnicos asociados a las plataformas de mensajería institucional y complementar dichas medidas con procesos permanentes de sensibilización.

El CSIRT Salud recomienda implementar las siguientes medidas:

- Configurar y mantener correctamente los mecanismos SPF, DKIM y DMARC para reducir los riesgos asociados con la suplantación de dominios institucionales.
- Fortalecer los filtros antispam y antimalware mediante mecanismos de análisis dinámico de archivos adjuntos y enlaces incluidos en los mensajes.
- Restringir la recepción de archivos ejecutables, scripts, macros y demás formatos considerados de alto riesgo cuando no exista una necesidad operacional debidamente justificada.
- Implementar mecanismos de reescritura y análisis de URL para identificar enlaces maliciosos antes de que sean accedidos por los usuarios.
- Desarrollar campañas periódicas de concientización sobre phishing, ingeniería social, smishing y otras modalidades de fraude digital dirigidas a funcionarios y contratistas.
- Realizar ejercicios controlados de simulación de phishing que permitan medir el nivel de madurez institucional y fortalecer la cultura de ciberseguridad.
- Establecer procedimientos claros para el reporte oportuno de mensajes sospechosos por parte de los usuarios y garantizar su atención por los equipos responsables de seguridad de la información.

Protección de estaciones de trabajo y servidores

Las estaciones de trabajo, servidores y demás equipos que soportan la operación institucional continúan siendo uno de los principales objetivos de los actores de amenaza para establecer persistencia, ejecutar código malicioso, realizar movimientos laterales y desplegar ataques de ransomware. Por esta razón, resulta fundamental fortalecer los controles de protección de los

equipos, priorizando mecanismos de prevención, detección temprana y respuesta automatizada frente a actividades sospechosas.

El CSIRT Salud recomienda implementar las siguientes medidas:

- Implementar soluciones de Detección y Respuesta en Endpoints (EDR) o Detección y Respuesta Extendida (XDR) que permitan identificar comportamientos anómalos.
- Mantener actualizados los sistemas operativos, aplicaciones y motores de seguridad mediante procesos formales de gestión de vulnerabilidades y aplicación oportuna de parches de seguridad.
- Restringir la ejecución de software no autorizado mediante listas de aplicaciones permitidas (Application Allowlisting) o mecanismos equivalentes.
- Deshabilitar servicios, protocolos y funcionalidades que no sean requeridos para la operación institucional, reduciendo la superficie de ataque de los equipos.
- Configurar mecanismos de protección contra ransomware que permitan identificar modificaciones masivas de archivos y ejecutar acciones automáticas de contención.
- Limitar el uso de privilegios administrativos locales, evitando que los usuarios operen permanentemente con cuentas de administrador.
- Implementar controles que permitan registrar y monitorear la ejecución de herramientas administrativas, intérpretes de comandos y lenguajes de automatización, como PowerShell, CMD o Bash, para identificar posibles usos maliciosos.

Protección de infraestructura tecnológica

La infraestructura tecnológica constituye el soporte fundamental para la prestación de los servicios de salud. Firewalls, dispositivos de seguridad perimetral, redes corporativas, servicios de acceso remoto, servidores, plataformas de virtualización y sistemas de almacenamiento deben mantenerse adecuadamente protegidos para reducir las posibilidades de acceso no autorizado y limitar la propagación de un incidente de seguridad.

El CSIRT Salud recomienda implementar las siguientes medidas:

- Mantener actualizados los dispositivos de seguridad perimetral, equipos de red, plataformas de virtualización y demás componentes de infraestructura mediante la aplicación oportuna de actualizaciones de seguridad.

- Restringir la exposición de servicios administrativos directamente hacia Internet, privilegiando el uso de VPN seguras y mecanismos robustos de autenticación.
- Implementar segmentación de red para separar los ambientes administrativos, asistenciales, biomédicos, invitados y demás zonas críticas de la organización.
- Revisar periódicamente las reglas de firewalls, listas de control de acceso (ACL) y políticas de filtrado para eliminar configuraciones obsoletas o innecesarias.
- Deshabilitar protocolos inseguros y restringir el uso de servicios de administración remota cuando no sean estrictamente necesarios.
- Implementar mecanismos de inspección del tráfico de red que permitan identificar comportamientos anómalos, conexiones sospechosas y posibles movimientos laterales dentro de la infraestructura.
- Verificar periódicamente la configuración de dispositivos de red, asegurando el uso de protocolos seguros para la administración y el cifrado de las comunicaciones.

Protección de servicios en la nube

La adopción de servicios en la nube ha permitido mejorar la disponibilidad y escalabilidad de múltiples procesos del sector salud; sin embargo, también ha ampliado la superficie de ataque de las organizaciones. Configuraciones inseguras, permisos excesivos, autenticaciones débiles y aplicaciones de terceros representan algunos de los principales riesgos identificados en incidentes recientes.

El CSIRT Salud recomienda implementar las siguientes medidas:

- Habilitar autenticación multifactor para todas las cuentas con acceso a plataformas de nube y servicios de colaboración institucional.
- Revisar periódicamente los permisos asignados a usuarios, grupos, aplicaciones y cuentas de servicio, aplicando el principio de mínimo privilegio.
- Monitorear continuamente las actividades administrativas, autenticaciones, cambios de configuración y accesos a información crítica almacenada en la nube.
- Restringir el uso de aplicaciones de terceros que soliciten permisos excesivos sobre la información institucional y revisar periódicamente las autorizaciones previamente otorgadas.
- Implementar mecanismos de prevención de pérdida de información (DLP) para proteger datos personales, información clínica y demás información sensible almacenada en plataformas de nube.

- Verificar periódicamente la configuración de repositorios de almacenamiento para evitar la exposición pública accidental de información institucional.
- Mantener procedimientos de respaldo y recuperación que contemplen la información almacenada en servicios de nube y permitan restaurar los servicios ante incidentes de seguridad o errores operacionales.

Protección de activos críticos del sector salud

Las entidades del sector salud administran activos tecnológicos cuya indisponibilidad, alteración o compromiso puede afectar directamente la prestación de los servicios asistenciales, la seguridad del paciente y la continuidad de la operación institucional. Sistemas como la Historia Clínica Electrónica (HCE), los Sistemas de Información Hospitalaria (HIS), los Sistemas de Información de Laboratorio (LIS), los Sistemas de Información Radiológica (RIS), los Sistemas de Archivo y Comunicación de Imágenes (PACS), las plataformas de telemedicina y los dispositivos médicos conectados (IoMT) requieren controles de seguridad adicionales debido al alto valor de la información que procesan y a su impacto sobre la atención en salud.

El CSIRT Salud recomienda implementar las siguientes medidas:

- Identificar y mantener actualizado el inventario de los activos tecnológicos críticos que soportan la prestación de servicios asistenciales, incluyendo sistemas clínicos, dispositivos biomédicos conectados y plataformas de apoyo diagnóstico.
- Implementar controles de acceso que garanticen que únicamente el personal autorizado pueda acceder a los sistemas clínicos, aplicando el principio de mínimo privilegio y mecanismos robustos de autenticación.
- Mantener actualizados los sistemas clínicos y dispositivos biomédicos de acuerdo con las recomendaciones de los fabricantes, evaluando previamente los posibles impactos sobre la continuidad del servicio asistencial.
- Segmentar las redes que soportan dispositivos médicos conectados y sistemas clínicos críticos, evitando su comunicación directa con redes administrativas o de acceso general.
- Restringir el acceso remoto a equipos biomédicos y plataformas clínicas únicamente a los casos estrictamente necesarios, utilizando conexiones seguras, autenticación multifactor y mecanismos de monitoreo continuo.
- Verificar periódicamente la integridad y disponibilidad de la información almacenada en los sistemas clínicos, asegurando la existencia de mecanismos de respaldo y

recuperación que permitan restablecer oportunamente la operación ante incidentes de ciberseguridad.

- Coordinar con proveedores de tecnología médica y desarrolladores de software clínico la gestión oportuna de vulnerabilidades, actualizaciones de seguridad y planes de respuesta frente a incidentes que puedan afectar los servicios asistenciales.

Monitoreo y detección de amenazas

La detección temprana constituye uno de los factores más importantes para reducir el impacto de un incidente de ciberseguridad. Las organizaciones que cuentan con capacidades de monitoreo continuo, correlación de eventos y análisis oportuno de alertas logran identificar actividades maliciosas en etapas tempranas del ataque, reduciendo significativamente la probabilidad de compromiso de activos críticos y la propagación dentro de la infraestructura tecnológica.

El CSIRT Salud recomienda implementar las siguientes medidas:

- Centralizar los registros de auditoría generados por servidores, estaciones de trabajo, dispositivos de seguridad, aplicaciones críticas y servicios en la nube para facilitar su análisis y correlación.
- Implementar mecanismos de monitoreo continuo que permitan identificar comportamientos anómalos relacionados con autenticaciones, elevación de privilegios, movimientos laterales, ejecución de código sospechoso y exfiltración de información.
- Supervisar permanentemente los accesos a cuentas privilegiadas y establecer alertas para detectar autenticaciones desde ubicaciones inusuales, horarios atípicos o múltiples intentos fallidos de autenticación.
- Monitorear los cambios realizados sobre configuraciones críticas de infraestructura, plataformas de nube, dispositivos de seguridad y sistemas clínicos.
- Establecer procedimientos para la revisión periódica de indicadores de compromiso (IoC), inteligencia de amenazas y boletines emitidos por organismos nacionales e internacionales de ciberseguridad.
- Verificar periódicamente el funcionamiento de las herramientas de monitoreo y asegurar la conservación de los registros de auditoría durante los periodos definidos por la organización y la normativa aplicable.
- Definir procedimientos de escalamiento que permitan atender oportunamente los eventos de seguridad clasificados como críticos o de alto impacto.

Preparación y respuesta ante incidentes de ciberseguridad

La capacidad para responder de manera oportuna frente a un incidente constituye un elemento fundamental para reducir su impacto operacional y facilitar la recuperación de los servicios afectados. Las entidades del sector salud deben contar con procedimientos previamente definidos que permitan coordinar las actividades de contención, análisis, recuperación y comunicación frente a eventos que comprometan la confidencialidad, integridad o disponibilidad de la información.

El CSIRT Salud recomienda implementar las siguientes medidas:

- Mantener actualizado el Plan de Respuesta a Incidentes de Seguridad de la Información, definiendo claramente los roles, responsabilidades, procedimientos de escalamiento y mecanismos de coordinación institucional.
- Verificar periódicamente la disponibilidad e integridad de las copias de seguridad mediante la realización de pruebas de restauración, priorizando los sistemas que soportan procesos críticos para la prestación de servicios de salud.
- Implementar estrategias de respaldo que contemplen copias desconectadas o inmutables para reducir el impacto de ataques de ransomware.
- Establecer procedimientos para el aislamiento oportuno de equipos comprometidos y la preservación de evidencias digitales que faciliten el análisis forense y la investigación del incidente.
- Realizar ejercicios periódicos de simulación que permitan validar la capacidad institucional para responder a incidentes de ciberseguridad y fortalecer la coordinación entre las áreas técnicas, asistenciales y administrativas.
- Mantener actualizados los canales de comunicación con el CSIRT Salud y demás autoridades competentes para facilitar el reporte oportuno de incidentes y el intercambio de información técnica.
- Incorporar las lecciones aprendidas derivadas de incidentes reales o ejercicios de simulación dentro de los procesos de mejora continua de la gestión de la seguridad de la información.

Recomendaciones para la Alta Dirección

La ciberseguridad constituye un elemento estratégico para garantizar la continuidad de los servicios de salud y proteger la información administrada por las entidades del sector. En consecuencia, la Alta Dirección debe liderar la gestión del riesgo cibernético, promoviendo la asignación de recursos, el fortalecimiento de las capacidades institucionales y la implementación de controles proporcionales al nivel de exposición de la organización.

El CSIRT Salud recomienda a los representantes legales, gerentes, directores, juntas directivas y demás responsables de la toma de decisiones considerar las siguientes acciones:

- Incorporar el riesgo cibernético dentro de los procesos institucionales de gestión del riesgo y continuidad del negocio.
- Promover la implementación de programas permanentes de sensibilización y capacitación dirigidos a funcionarios, contratistas y terceros.
- Supervisar periódicamente el estado de implementación de los controles de seguridad y los planes de tratamiento de riesgos asociados a los activos críticos.
- Verificar que la organización disponga de procedimientos para la gestión de incidentes, continuidad del negocio y recuperación ante desastres.
- Promover ejercicios periódicos de simulación de incidentes de ciberseguridad que involucren tanto a las áreas técnicas como a los responsables de la toma de decisiones.
- Fomentar una cultura organizacional orientada a la protección de la información, el cumplimiento de las políticas institucionales y el reporte oportuno de eventos e incidentes de seguridad.

Lista de verificación para el fortalecimiento de la postura de ciberseguridad

Como mecanismo de apoyo para las entidades del sector salud, el CSIRT Salud presenta la siguiente lista de verificación, la cual puede ser utilizada para identificar oportunidades de mejora y priorizar la implementación de controles de seguridad:

Tabla 1. Lista de Verificación de la postura de seguridad

Control	SÍ	NO	N/A
Se encuentra implementada autenticación multifactor para usuarios privilegiados.			
Las cuentas de usuarios retirados son deshabilitadas oportunamente			
Se realizan revisiones periódicas de privilegios de acceso			

Control	SÍ	NO	N/A
El correo electrónico cuenta con controles SPF, DKIM, DMARC			
Se ejecutan campañas periódicas de sensibilización sobre phishing			
Las estaciones de trabajo cuentan con soluciones EDR y XDR			
Existe un proceso formal de gestión de vulnerabilidades y aplicación de parches			
La infraestructura tecnológica se encuentra segmentada de acuerdo con el nivel de criticidad			
Los servicios críticos expuestos a internet utilizan autenticación multifactor			
Se monitorean continuamente los eventos de seguridad de los activos críticos			
Se realizan copias de seguridad periódicas y pruebas de restauración			
Se cuenta con plan de respuesta a incidentes actualizado			
Se encuentran identificados los activos tecnológicos críticos del sector salud			
Se monitorean permanentemente las plataformas de nube utilizadas por la entidad			
Se han realizado ejercicios de simulación de incidentes durante el último año			

Fuente: CSIRT Salud, 2026

Nota: La presente lista constituye una herramienta de autoevaluación y no reemplaza los procesos de auditoría, evaluación de riesgos o verificación de cumplimiento que cada entidad deba realizar conforme a su marco normativo y a sus políticas institucionales.

Recomendaciones finales

El incremento de los ataques dirigidos contra entidades públicas e infraestructuras críticas evidencia que la ciberseguridad debe abordarse como un proceso permanente de gestión del riesgo y no únicamente como una respuesta frente a incidentes específicos. La evolución constante de las tácticas, técnicas y procedimientos empleados por los actores de amenaza exige que las organizaciones mantengan un proceso continuo de fortalecimiento de sus capacidades de prevención, detección, respuesta y recuperación.

Las entidades del sector salud administran información altamente sensible y prestan servicios esenciales para la población, razón por la cual deben priorizar la implementación de controles que contribuyan a reducir la superficie de exposición, proteger los activos críticos y fortalecer la resiliencia institucional frente a eventos de ciberseguridad.

El CSIRT Salud invita a las entidades que conforman su comunidad a evaluar las recomendaciones presentadas en este boletín, priorizar aquellas que resulten aplicables de acuerdo con su nivel de madurez y adoptar un proceso de mejora continua que permita fortalecer progresivamente su postura de ciberseguridad.

Ante la identificación de eventos o incidentes que puedan comprometer la confidencialidad, integridad o disponibilidad de la información, se recomienda realizar el reporte oportuno al CSIRT Salud a través de los canales institucionales establecidos, con el fin de facilitar el análisis técnico, la correlación de eventos y el apoyo durante las actividades de contención y recuperación.

Fuentes:

- <https://www.nist.gov/cyberframework>
- <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
- <https://csrc.nist.gov/publications/detail/sp/800-207/final>
- <https://www.cisecurity.org/controls>
- <https://attack.mitre.org>
- <https://www.first.org/tlp>
- <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>
- <https://www.cisa.gov/shields-up>
- <https://www.enisa.europa.eu>
- <https://www.iso.org/standard/82875.html>
- <https://www.iso.org/standard/75652.html>
- <https://www.microsoft.com/security/security-insider/microsoft-digital-defense-report>
- <https://www.reuters.com/legal/government/colombias-ecopetrol-says-cyberattack-stole-data-tied-3300-accounts-2026-07-18/>
- <https://www.nist.gov/news-events/news/2026/06/now-available-practical-guidelines-preventing-and-mitigating-ransomware>

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.