Alerta ID:	089
Fecha del reporte:	05/05/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Fuga de Datos y Acceso No Autorizado Hospital Universitario Nacional de Colombia
Herramienta de detección	N/A
Activo involucrado:	sistemas expuestos a internet
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Alta

Resumen ejecutivo

Informar a las entidades sobre el presunto compromiso del Hospital Universitario Nacional de Colombia (HUN – hun.edu.co), reportada el 2 de mayo de 2026 por el actor de amenaza 'macaroni'.

El HUN es una entidad de alta complejidad adscrita académicamente a la Universidad Nacional de Colombia, con presencia critica en la prestación de servicios de salud especializados. Una brecha de esta magnitud representa un riesgo directo para la privacidad de los pacientes, la continuidad operacional del hospital y el cumplimiento normativo bajo la legislación colombiana (Ley 1581 de 2012 - Habeas Data).

Descripción:

El día 2 de mayo de 2026, el actor de amenaza identificado bajo el alias macaroni público en un foro de cibercrimen de la dark web (indexado por Dark Web Informer / CIAC) una oferta de venta que incluía:

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Un volcado completo (full DB dump) de 8 bases de datos del Hospital Universitario Nacional de Colombia.
- 197 tablas de datos comprometidas provenientes del servidor de producción.
- Acceso en vivo y confirmado (live access) al servidor de producción del hospital, el cual aún se encontraba operacional y accesible públicamente al momento de la publicación.

El post fue publicado aproximadamente a las 11:22 AM y editado 1 vez en total, con la descripción: "Complete database dump from the Hospital Universitario Nacional de Colombia (hun.edu.co). Extracted TODAY (May 2, 2026) from a production server that is still running and accessible on the internet."

El perfil indica un actor relativamente nuevo, pero con alta reputación acumulada rápidamente, lo que sugiere experiencia previa o cooperación con otros actores del ecosistema criminal. La categoría "MVP User" en estos foros generalmente se obtiene mediante contribuciones valoradas por la comunidad, como la provisión de datos validos o accesos verificados.

Modo de explotación detallado.

Dado que el actor confirma extracción directa desde un servidor de producción "accesible en internet", el vector de ataque más probable sigue la siguiente cadena de explotación:

Fase 1: Reconocimiento (Reconnaissance)
El atacante realizo un reconocimiento activo o pasivo del dominio hun.edu.co para identificar activos expuestos en Internet. Las técnicas probablemente empleadas incluyen:

- Escaneo de puertos con herramientas como Shodan, Censys o Nmap para identificar servicios de base de datos expuestos (MySQL:3306, MSSQL:1433, PostgreSQL:5432, MongoDB:27017).
- Enumeración de subdominios y paneles de administración web (phpMyAdmin, Adminer, pgAdmin) accesibles públicamente sin autenticación robusta.
- Búsqueda de credenciales filtradas en brechas anteriores asociadas al dominio hun.edu.co en repositorios como Pastebin, GitHub o foros de la dark web.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Análisis de metadatos en documentos públicos del sitio web para identificar versiones de software, usuarios internos y tecnologías utilizadas.

Fase 2: Acceso Inicial (Initial Access)

Una vez identificado el vector, el atacante pudo haber obtenido acceso mediante una o varias de las siguientes técnicas:

- Credenciales débiles o por defecto: servidores de bases de datos con contraseñas triviales (root/root, admin/admin, sa/sa) expuestos directamente a Internet.
- SQL Injection: explotación de vulnerabilidades de inyección SQL en aplicaciones web del hospital para obtener credenciales de base de datos o acceso directo.
- Exposición directa de puertos de BD a Internet: puertos de base de datos accesibles sin firewall, VPN ni lista de control de acceso (ACL), permitiendo conexiones directas desde cualquier IP.
- Reutilización de credenciales (Credential Stuffing): uso de combinaciones usuario/contraseñas obtenidas de filtraciones anteriores de datos colombianos (DIAN, ICFES, SDS) para autenticarse en los sistemas del HUN.
- Vulnerabilidades en paneles de administración web (phpMyAdmin sin autenticación o con versión desactualizada vulnerable a RCE).

Fase 3: Exfiltración de Datos (Exfiltration)

Con acceso autenticado a la base de datos, el atacante ejecuto la extracción masiva:

- Uso de utilidades nativas de exportación: mysqldump -u root -p --all-databases > dump.sql o equivalente para cada motor de base de datos.
- Consultas SELECT masivas con exportación a CSV o JSON mediante INTO OUTFILE o clientes gráficos de BD.
- Transferencia de los archivos resultantes a infraestructura externa controlada por el atacante mediante FTP, SCP, o servicios de almacenamiento anónimo.
- El hecho de que el acceso sea "en vivo" al momento de la publicación indica que el atacante mantuvo persistencia en el servidor, posiblemente mediante un usuario de BD backdoor, una web shell o una tarea programada (cron job).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fase 4: Monetización (Explotacion Financiera)

- El actor público el dump y el acceso en vivo como un paquete a la venta en el foro de cibercrimen, ofreciendo a compradores potenciales tanto los datos históricos como capacidad operacional continua sobre el servidor de producción.
- Este modelo de doble venta (datos + acceso) maximiza el retorno económico del ataque y aumenta exponencialmente el riesgo para la organización víctima.

Indicadores de compromiso

Con base en la información disponible en la publicación del actor y patrones típicos de este tipo de ataques, se identifican los siguientes indicadores de compromiso probables:

IOCs de Red

- Trafico anómalo en los puertos 3306 (MySQL), 5432 (PostgreSQL), 1433 (MSSQL) o 27017 (MongoDB) accesibles desde Internet sin restricción de IP.
- Consultas masivas tipo SELECT * FROM o mysqldump / pg_dump desde IPs externas o no autorizadas.
- Sesiones de base de datos activas desde geolocalizaciones inusuales (fuera de Colombia o de la red corporativa).

IOCs de Host

- Presencia de herramientas de exfiltración: mysqldump, pg_dump, sqlcmd, DataGrip, DBeaver, scripts .sh o .py con conexiones a BD externas.
- Archivos .sql, .csv o .zip de gran tamaño creados recientemente en directorios temporales (/tmp, C:\Temp).
- Cuentas de usuario de base de datos con permisos elevados creadas recientemente o con patrones de nombre inusuales.
- Registros de acceso en logs de bases de datos con comandos de exportación masiva o creación de usuarios backdoor.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

IOCs Contextuales

- Alias del actor: macaroni (monitorear en foros de cibercrimen: BreachForums, XSS, Exploit.in, RaidForums mirrors).
- Hash o muestra de los datos publicados como prueba de exfiltracion en el hilo original del foro.
- Presencia del dominio hun.edu.co en listas de monitoreo de fugas de datos (HaveIBeenPwned, DeHashed, IntelX).

Vulnerabilidades.

CVE-1: Exposición Directa de Servicios de Base de Datos a Internet
Descripción: Puertos de gestión de bases de datos (3306, 5432, 1433, 27017) accesibles desde Internet sin restricción de origen. Este es el vector más crítico y probablemente el principal utilizado en este ataque.

Severidad: CRITICA (CVSS v3: 9.8 si no requiere autenticación, 8.8 si requiere credenciales débiles).
Impacto: Permite a cualquier actor en Internet intentar autenticación directa contra la base de datos, sin necesidad de comprometer capas adicionales de la infraestructura.

CVE-2: Credenciales Débiles o por Defecto en Sistemas de Base de Datos
Descripción: Uso de contraseñas triviales o por defecto en cuentas administrativas de bases de datos (root, sa, admin, postgres).
Severidad: CRITICA. La combinación con la exposición de puertos crea un vector de ataque directo y de muy bajo costo técnico para el atacante.
Referencia: CWE-521 (Weak Password Requirements), CWE-798 (Use of Hard-coded Credentials).

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

CVE-3: Falta de Segmentación de Red y Controles de Acceso
Descripción: Ausencia de firewall perimetral o reglas de segmentación que limiten el acceso a servicios de base de datos únicamente desde servidores de aplicación internos autorizados.
Severidad: ALTA. La segmentación de red es un control fundamental para limitar la superficie de ataque de activos críticos como las bases de datos hospitalarias.

CVE-4: Posible SQL Injection en Aplicaciones Web
Descripción: Si el vector de acceso inicial fue a través de la capa de aplicación web, podrían existir vulnerabilidades de inyección SQL no parcheadas en los portales del hospital (portal de pacientes, sistema de citas, intranet).
Severidad: ALTA-CRITICA según el nivel de privilegios obtenibles. Referencia: CWE-89 (SQL Injection), OWASP Top 10 - A03:2021.

CVE-5: Falta de Monitoreo y Alertas sobre Actividad Anómala en BD
Descripción: La ausencia de sistemas de detección de anomalías en la capa de base de datos permitió que el atacante realizara consultas masivas de exportación sin disparar alertas ni activar mecanismos de respuesta automática.
Severidad: MEDIA-ALTA como control preventivo. Su ausencia eleva el impacto de todas las vulnerabilidades anteriores al no permitir detección temprana.

Principales activos afectados.

Con base en los datos disponibles en la publicación y el perfil técnico común de infraestructuras hospitalarias colombianas, los siguientes activos se consideran potencialmente afectados:

Sistemas de Base de Datos

- Motor de BD: MySQL 5.x/8.x, MariaDB, Microsoft SQL Server 2014-2019, PostgreSQL 9.x-14.x (por determinar versión exacta).
- Esquema: 8 bases de datos independientes con 197 tablas en total. La escala sugiere un sistema HIS (Hospital Information System) complejo o múltiples aplicaciones integradas.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Datos probablemente contenidos: registros de pacientes (HCE - Historia Clínica Electrónica), datos demográficos, diagnósticos CIE-10, prescripciones, resultados de laboratorio, imágenes diagnosticas (metadata), facturacion RIPS, credenciales de usuarios del sistema.

Servidor de Producción

- Sistema Operativo: Linux (Ubuntu/CentOS probable) o Windows Server (por determinar).
- El servidor es accesible directamente desde Internet, lo que indica ausencia de WAF (Web Application Firewall) o firewall de aplicación de BD efectivo.

Aplicaciones Potencialmente Comprometidas

- Portal de pacientes (cocoreservas.com/HUN) - sistema de citas online.
- Sistema de información hospitalaria (HIS/RIS/LIS) interno.
- Plataforma de formación virtual (formacion.hun.edu.co).
- Sistemas de radiología e imágenes diagnosticas (PACS/RIS).

Recomendaciones

- AISLAMIENTO: Bloquear INMEDIATAMENTE todo acceso externo a puertos de bases de datos (3306, 5432, 1433, 27017, 5984, 6379, 9200) en el firewall perimetral.
- REVOCACION DE CREDENCIALES: Cambiar TODAS las contraseñas de usuarios de bases de datos, especialmente cuentas root/admin/sa. Revocar tokens y certificados de acceso activos.
- AUDITORIA DE ACCESOS: Revisar logs de acceso de BD de las últimas 72 horas para identificar IPs externas, consultas masivas (SELECT *, mysqldump), y creación de nuevos usuarios.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fuentes:

- Dark Web Informer – Leak ICFES Colombia — https://darkwebinformer.com/alleged-data-leak-exposes-30-million-colombian-citizens-from-icfes-national-education-database/
- DeXpose.io – Ransomware Hospital del Sur Colombia — https://www.dexpose.io/thegentlemen-strike-hospital-del-sur-in-colombia-ransomware-attack/
- BreachSense – Data Breach News 2026 — https://www.breachsense.com/breaches/
- Brinztech – Leak Universidad Santiago de Cali — https://www.brinztech.com/breach-alerts/brinztech-alert-alleged-database-leak-of-universidad-santiago-de-cali-usc
- Darknetsearch – DIAN Data Leak — https://darknetsearch.com/knowledge/news/en/dian-data-leak-revealed-7-key-facts-you-must-know/
- CybelAngel – The Dark Web in 2026 — https://cybelangel.com/blog/dark-web-guide-2026/
- Palo Alto Networks – Dark Web Leak Sites — https://www.paloaltonetworks.com/cyberpedia/what-is-a-dark-web-leak-site

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) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570