# UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO FACULTAD DE ESTUDIOS SUPERIORES ARAGON

**INGENIERIA EN COMPUTACIÓN 9NO SEMESTRE SEGURIDAD INFORMATICA.**

# FILTRACION DE DATOS DEL IMSS.

**JOSE NESTOR LÓPEZ PADILLA.**

GRUPO: 1907

## Introducción:

En septiembre de 2025 surgieron reportes de que una base de datos con información de 20 millones de pensionados del Instituto Mexicano del Seguro Social (IMSS) estaba a la venta en foros de la dark web, la filtración incluiría datos personales y médicos sensibles. La aparición del archivo provocó investigaciones y declaraciones públicas por parte de las empresas de seguridad y el propio IMSS, que niega un “hackeo” directo a sus sistemas.

Ahora para tratar de tener una idea más clara de lo sucedido, investigue un poco de como fue que sucedieron los hechos, guiándome por las fechas:

**12 de septiembre de 2025 (aprox.):** Primeras señales en la dark web y foros clandestinos sobre la venta de una base de datos llamada algo así como “IMSS Pensionados 2025”. Expertos en ciberseguridad y periodistas comenzaron a detectar la publicación.

**23–29 de septiembre de 2025:** Varios medios y cuentas especializadas reportan que el archivo (aproximadamente de 1.4 GB) contiene datos de alrededor de 20 millones de registros (nombres, direcciones, CURP, NSS, fechas de nacimiento, padecimientos y tipos de sangre). Se afirma que la información apareció a la venta y que el precio ofrecido en algunos anuncios era de 50,000 pesos aproximadamente.

**24–30 de septiembre / principios de octubre 2025**: El IMSS emite comunicados negando que exista evidencia de una intrusión directa a su infraestructura, habla de “uso indebido por parte de personal” y anuncia investigación interna. Los medios publican análisis y comentarios de especialistas en seguridad.

Sin embargo, algo que pude notar es que hay irregularidades en la información pública, pues mientras varios grupos de ciberseguridad y periodistas hablan de venta o filtración, el IMSS afirma que no hay evidencia de hackeo directo a sus sistemas, y esto complica la atribución de la culpa, pero define parte de la respuesta que da el IMSS.

## Problemática:

Estamos hablando de un tema bastante delicado y preocupante, pues se trata de robo de identidad y fraude, con NSS, CURP y datos personales que facilitan clonaciones de identidad, solicitudes fraudulentas de crédito, trámites de seguridad social, etc.

Con la exposición de datos médicos se puede llegar a usar para discriminación, chantaje o explotación comercial (publicidad orientada, tráfico de datos clínicos), riesgo reputacional y pérdida de confianza, pues los usuarios y derechohabientes pierden confianza en la institución (aún más).

Ahora, si se llega a demostrar negligencia en el tratamiento de datos personales conforme a la normativa mexicana e internacional, indudablemente harán sanciones fuertes, legales y regulatorias.

Dado que las fuentes independientes como los periodistas y empresas de ciberseguridad, han encontrado anuncios y copias del supuesto dataset en foros de la dark web y lo han divulgado públicamente. Y que según las declaraciones del IMMS no hay evidencia de intrusión a su infraestructura y que investigan “uso indebido por parte de personal” o fuentes internas, no hay una respuesta clara por ninguno de los dos lados, por lo tanto, yo creo que existen dos narrativas: filtración externa o filtración interna.

Que versión es la verdadera sería la pregunta ante esta situación.

## Acciones Correctivas y preventivas.

Creo que lo ideal es empezar por una investigación forense digital completa.

1. Contratar un equipo externo al IMSS especializado en ciberseguridad para realizar un análisis forense de los sistemas, registros de acceso, logs, tráfico de red, puntos de salida de datos. Determinar cómo se extrajo la información y ver las vulnerabilidades, credenciales robadas, el acceso interno, error humano, proveedor externo, etc.
2. Preservar evidencia digital (imágenes forenses de servidores, backups, registros de acceso) para posibles responsabilidades legales y sanciones.
3. Contención del incidente y remediación de acceso, identificando y aislando los sistemas afectados o comprometidos (bases de datos, servidores de acceso remoto, repositorios internos) para detener la fuga de datos.
4. Revocar y cambiar todas las credenciales (ya sean las de los administradores, servicio, cuentas de acceso externo, todas).
5. Revisar y parchear todas las vulnerabilidades conocidas de los sistemas (sistemas operativos, bases de datos, conectividad externa, APIs).
6. Ofrecer mecanismos de monitoreo de identidad, alertas de fraude y recomendaciones a los usuarios para revisar sus estados financieros y reportar irregularidades.
7. Segmentar la red del IMSS de tal forma que las bases de datos sensibles (como NSS, CURP, historiales médicos) estén en zonas de red altamente restringidas, con mínimo acceso externo.
8. Implementar bastion hosts, jump-servers para cualquier acceso administrativo, y evitar accesos directos desde redes menos seguras.
9. Gestionar adecuadamente las claves de cifrado con políticas de rotación de claves y control de acceso al módulo de cifrado.
10. Asegurar que todos los datos personales y médicos estén cifrados tanto cuando se almacenan como cuando se transmiten entre sistemas.
11. Establecer controles estrictos para accesos remotos, uso de cuentas administrativas y registro de sesiones.
12. Monitorear continuamente la detección de exfiltración (DLP) e inteligencia de amenazas.
13. Instalar soluciones de DLP que detecten patrones de salida de datos sensibles (como exportaciones masivas de CSV, envíos por FTP, uploads sospechosos).
14. Implementar sistemas de detección de amenazas y anomalías de comportamiento para identificar accesos inusuales o grandes volúmenes de lectura/exportación de datos.
15. Establecer un programa permanente de seguridad informática, con simulaciones (phishing interno, ejercicios de respuesta) y sanciones claras por incumplimiento.
16. Revisar los contratos con proveedores que tengan acceso a datos sensibles, exigir certificaciones de seguridad (por ejemplo, ISO 27001), auditorías regulares y cláusulas de responsabilidad.
17. Limitar el acceso de terceros, usar contratos de confidencialidad, acceso granular y monitoreo de sus actividades.
18. Asegurar que existan backups cifrados y fuera de línea de los sistemas críticos, pruebas regulares de restauración y un plan de incidente actualizado.
19. Simular regularmente incidentes de seguridad para evaluar tiempos de reacción, coordinación entre unidades, y comunicación hacia afectados.
20. Realizar auditorías internas y externas de seguridad informática, revisiones de cumplimiento con la normativa de datos personales en México, y seguimiento de vulnerabilidades.
21. Registrar métricas de seguridad (tiempo medio de detección, número de incidentes, número de accesos privilegiados revocados, etc.) y reportarlas a la alta dirección.

Notificar a las autoridades de ciberseguridad y protección de datos:

1. Notificar al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y a la autoridad legal

correspondiente para cumplimiento de la normativa de protección de datos personales.

1. Coordinar con las fuerzas de seguridad cibernética para rastrear la fuente del incidente, posibles actores maliciosos y mitigar la propagación de los datos en la dark-web.