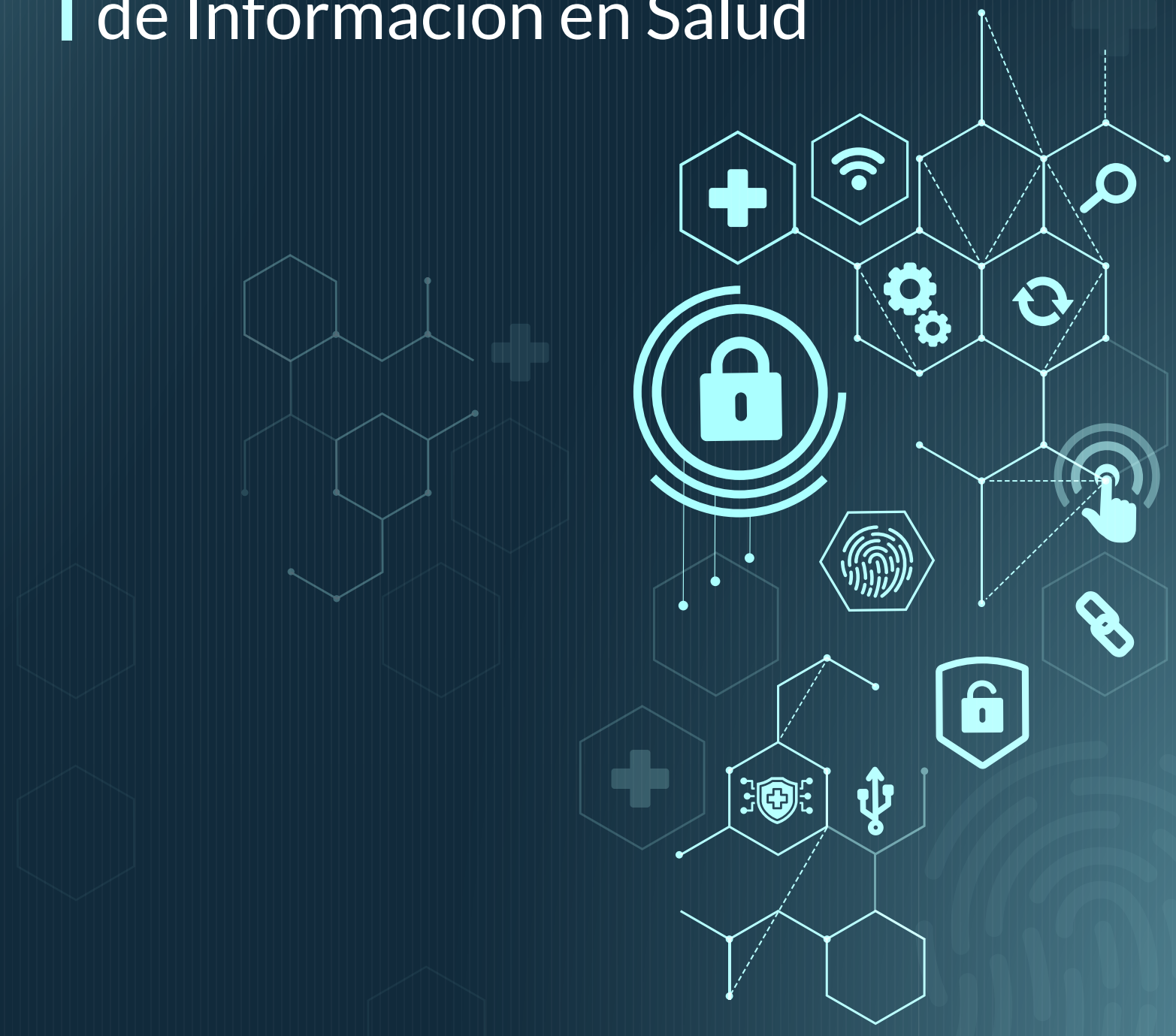
CENS
CENTRO NACIONAL EN SISTEMAS DE INFORMACIÓN EN SALUD

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

Recomendaciones de Ciberseguridad para Sistemas de Información en Salud



Introducción

Los sistemas de información en salud son uno de los principales blancos de los ciberataques a nivel mundial. Según el Banco Interamericano de Desarrollo (BID), desde 2019 el sector salud ha sufrido los ataques más graves y las vulneraciones pueden tardar hasta 329 días en detectarse, exponiendo información altamente sensible y afectando la continuidad de la atención (1).

En Chile, expertos advierten que las principales amenazas son el robo de datos personales de pacientes y la interrupción de los servicios clínicos, lo que incluso puede poner en riesgo la seguridad de las personas. Frente a este escenario, el Centro Nacional en Sistemas de Información en Salud (CENS) desarrolló un sello para evaluar la calidad de las plataformas de salud digital, incorporando la ciberseguridad como uno de sus ejes principales.

La ciberseguridad exige una vigilancia permanente debido a la constante evolución de las amenazas. Además, los pacientes tienen escasas herramientas para conocer si los sistemas que almacenan su información cumplen estándares adecuados de protección, pese a que el resguardo de sus datos constituye un derecho.

En los últimos años, Chile ha fortalecido su marco regulatorio con la promulgación de la Ley 21.459 sobre delitos informáticos (2) y el avance de la Ley 21.663, Marco de Ciberseguridad (3), que contempló la creación de la Agencia Nacional de Ciberseguridad (ANCI). El objetivo de la ANCI es proteger la infraestructura crítica y los servicios esenciales del país frente a amenazas digitales, estableciendo estándares obligatorios tanto para el sector público como privado, fortaleciendo la prevención, la gestión de riesgos y la cooperación frente al cibercrimen.

Chile presenta una alta adopción de registros clínicos electrónicos, con más del 70% de cobertura en el sistema público y más del 85% en el privado. Por ello, fortalecer la ciberseguridad se ha convertido en un requisito fundamental para proteger la información de los pacientes, asegurar la continuidad de la atención y consolidar la transformación digital del sistema de salud.

Para fortalecer la ciberseguridad, CENS y ANCI presentan estas recomendaciones, elaboradas a partir de los lineamientos técnicos y las alertas de amenazas emitidas por la Agencia Nacional de Ciberseguridad, incorporando los aprendizajes obtenidos del monitoreo realizado por el equipo técnico de la ANCI, de incidentes que afectan al sector salud. Su objetivo es traducir estos criterios en medidas concretas y aplicables a las instituciones que conforman el ecosistema de salud digital, contribuyendo a una gestión de la ciberseguridad más ordenada y coherente con el marco normativo vigente, así como alineada con los estándares promovidos por la Agencia a nivel nacional.

Recomendaciones de Seguridad de la Información

Para evitar que los datos de sus sistemas informáticos sean usados por grupos de amenaza, se recomienda como medida principal registrar al encargado o delegado de ciberseguridad de la institución en https://portal.anci.gob.cl. Este registro agiliza el reporte de incidentes de efecto significativo en caso de sufrir uno en el futuro y para recibir alertas sectoriales de inteligencia de amenazas con recomendaciones para evitar ser afectado por campañas maliciosas. El registro solo requiere de ClaveÚnica y permite reportar inmediatamente, mientras que la validación de los encargados para recibir información de inteligencia requiere de documentos firmados electrónicamente por el representante legal de la institución.

Las medidas técnicas y organizacionales que se presentan a continuación se organizan según la tríada CID, el modelo base de la seguridad de la información, que orienta la protección de la información en salud y los activos que la soportan. Su nombre proviene de tres principios clave: confidencialidad, integridad y disponibilidad. En conjunto, estos principios buscan asegurar que la información clínica sea accedida solo por quienes corresponde, que se mantenga correcta y completa, y que esté disponible cuando se necesita para la atención, la gestión y/o toma de decisiones.

Confidencialidad: significa que los datos de salud deben ser protegidos frente a accesos no autorizados. Esto implica aplicar controles como autenticación, perfiles de acceso y cifrado, resguardando así la privacidad de pacientes y equipos de salud.

Integridad: implica que la información debe mantenerse exacta, completa y sin alteraciones indebidas. En salud, esto es crítico porque una modificación, pérdida o error en un dato clínico puede afectar diagnósticos, tratamientos y decisiones sanitarias.

Disponibilidad: significa que los datos y sistemas deben estar accesibles cuando se requieren. Esto incluye contar con infraestructura, respaldos, continuidad operacional y planes de recuperación que permitan sostener la atención incluso ante fallas técnicas o incidentes.

Confidencialidad

Control de Acceso

- Implementar un sistema de control de acceso que contemple autorización por individuo autenticado, autorización basada en roles y membresía de grupos, y centralización de la autenticación a través de un sistema que emita credenciales válidas entre múltiples sistemas, respaldado por una matriz de roles documentada y actualizada. En caso de que una institución opere con múltiples sistemas, se debe centralizar la identidad mediante una única cuenta por usuario.

Identificación de Entidades

- Se recomienda que el sistema asigne un ID único a cada suplantado (entidad no verificada) antes de iniciar el proceso de autenticación, siguiendo el modelo Identificación, Autenticación, Autorización (IAA).

Restricción de Acceso

- Limitar cuando sea posible el acceso público desde Internet a plataformas que contengan datos médicos. Ejemplo de implementación: geofencing a nivel de firewall, listas de IPs habilitadas para conexión.
- Limitar el acceso a APIs a cuentas de usuario específicas, usando tokens revocables del lado del servidor o de corta duración.
- Implementar mecanismos de MFA en todas las cuentas con acceso público a datos de salud, activándolos de forma obligatoria al menos en cuentas que presenten comportamientos sospechosos.
- Limitar la duración de las sesiones de los usuarios (Timeout), considerando la duración de los turnos de trabajo y sin solicitar autenticación más de una vez al día.
- Tener sesiones basadas en cookies, estas deben ser inhabilitadas de forma centralizada a más tardar a las 24 hrs de su creación.
- Tener sesiones con JSON Web Token (JWT) u otras tecnologías descentralizadas: tokens de acceso con duración máxima de 15 minutos y tokens de actualización (refresh tokens) con duración máxima de un día.
- Bloquear o auditar preventivamente a los usuarios que no se han conectado en más de tres meses.
- Contar con cuentas de acceso individualizadas por usuario, evitando la creación de cuentas genéricas para prevenir el uso compartido de credenciales.
- Limitar el uso de contraseñas débiles en sistemas con cuentas de usuario accesibles desde Internet.

Gestión de Contraseñas

- Establecer contraseñas que exija su confidencialidad, prohíba el uso de contraseñas predeterminadas y establezca requisitos mínimos de complejidad (longitud, mayúsculas, minúsculas, números, caracteres especiales e impersonalidad), prohibiendo su reutilización entre sistemas y estableciendo cambios periódicos obligatorios, complementado con el uso de un gestor de contraseñas.

Criptografía

- Utilizar cifrado simétrico (AES) y/o asimétrico (RSA) como base para proteger datos sensibles, complementado con métodos avanzados según el contexto: criptografía de umbral para llaves maestras y backups críticos, criptografía basada en identidad para cifrado sin certificado previo, criptografía basada en certificados TLS para comunicaciones y firma de documentos clínicos, criptografía sin certificados en entornos donde una Public Key Infrastructure o Infraestructura de Clave Pública (PKI) centralizada sea inviable, y criptografía de clave aislada mediante dispositivos como por ejemplo: smartcard con PKCS.

Integridad

Gestión de Datos

- Establecer un proceso formal de gestión de datos que contemple la identificación y clasificación de datos sensibles, el registro de su ubicación y control de accesos, la definición de propietarios y sus responsabilidades, y la evaluación periódica de la vigencia de los datos, eliminando los obsoletos y protegiendo los que deban persistir.

Manejo de Errores en Datos

- Automatizar y estandarizar el manejo de errores en los datos, designando una persona responsable con los accesos y permisos necesarios para ejecutar el proceso de corrección.

Trazabilidad

- Llevar registro de todas las acciones de consulta sobre datos sensibles, indicando fecha y hora del evento, ID del usuario que realiza la consulta, RUT del usuario consultado y datos extraídos.
- Bloquear o auditar preventivamente a los usuarios que no se han conectado en más de tres meses.
- Contar con cuentas de acceso individualizadas por usuario, evitando la creación de cuentas genéricas para prevenir el uso compartido de credenciales.
- Limitar el uso de contraseñas débiles en sistemas con cuentas de usuario accesibles desde Internet.

Disponibilidad

Gestión de Riesgos

- Implementar un proceso de gestión de riesgos que contemple la identificación y priorización de componentes críticos del sistema, la evaluación de vulnerabilidades y su impacto potencial, y el desarrollo de planes de control que incluyan estrategias de defensa, mitigación y respuesta a incidentes.

Monitoreo

- Monitorear la creación y el uso de tokens y sesiones; ante consultas masivas o provenientes de IPs sospechosas, bloquear preventivamente los tokens y las cuentas asociadas.
- Configurar, cuando sea posible, alertas automáticas cuando un usuario ejecute un número elevado de consultas en un corto periodo de tiempo.

Estas recomendaciones responden a un escenario de riesgo dinámico, que requiere fortalecer las capacidades de prevención y respuesta de las instituciones de salud. Como parte de su labor de monitoreo, la ANCI ha identificado nuevas formas de ataque dirigidas a sistemas digitales vinculados al sector salud.

Amenazas detectadas

El Equipo del CSIRT Nacional de la Agencia Nacional de Ciberseguridad ha detectado campañas activas de actores de amenaza, los que están enfocados en usar cuentas de usuarios legítimos en sistemas digitales con integraciones a datos de salud sensibles, para la extracción y consulta en línea de esta información.

Lo anterior ha requerido contactar a un gran número de instituciones con credenciales filtradas por acción de infostealers, solicitando su bloqueo preventivo para limitar el acceso de estos grupos de amenaza. Asimismo, se ha solicitado a los servicios de salud públicos el pedir a sus proveedores que cuenten con controles tecnológicos que dificulten el éxito de los patrones de comportamiento de los atacantes. Si usted es un prestador de servicios digitales de un servicio público o privado y requiere contar con una lista de credenciales de usuarios detectada en la Dark Web, por favor regístrese en el Portal de la Agencia (https://portal.anci.gob.cl) y envíe un correo electrónico desde su cuenta institucional a ayuda@anci.gob.cl pidiendo esta información.

Conclusión

La ciberseguridad requiere un trabajo permanente y continuo. Las amenazas evolucionan constantemente, por lo que las instituciones deben estar preparadas para responder ante posibles incidentes. Para ello, es fundamental revisar los sistemas de manera periódica y fortalecer las medidas de protección, considerando que, aunque existan controles implementados, el riesgo nunca será cero.

Estas recomendaciones abordan algunos de los principales desafíos presentes en el ecosistema de salud digital, como el robo de credenciales y los accesos no autorizados a datos de pacientes. Su implementación no requiere necesariamente grandes inversiones, sino principalmente un compromiso institucional con la adopción de buenas prácticas de seguridad.

Avanzar en estas medidas permite proteger la continuidad de la atención, fortalecer la confianza de los pacientes en los sistemas de información en salud y evitar multas por no notificar en los plazos establecidos.

Referencias

1. Alzuri, P., Cabral Berenfus, F., Paz, S., Nowersztern, A. y Libedinsky, P. (2021). Protegiendo la salud digital: una guía de ciberseguridad en el sector de salud. Banco Interamericano de Desarrollo. https://doi.org/10.18235/0003741

2. Ministerio del Interior y Seguridad Pública (2022). Ley 21.459: Establece normas sobre delitos informáticos. Biblioteca del Congreso Nacional de Chile. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1177743

3. Ministerio del Interior y Seguridad Pública (2024). Ley 21.663: Ley Marco de Ciberseguridad. Biblioteca del Congreso Nacional de Chile. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1202434