SONICWALL

RESUMEN EJECUTIVO

Desafíos y complejidad de la transformación en la ciberseguridad sanitaria

Los cuatro problemas cruciales que afectan actualmente al sector sanitario.

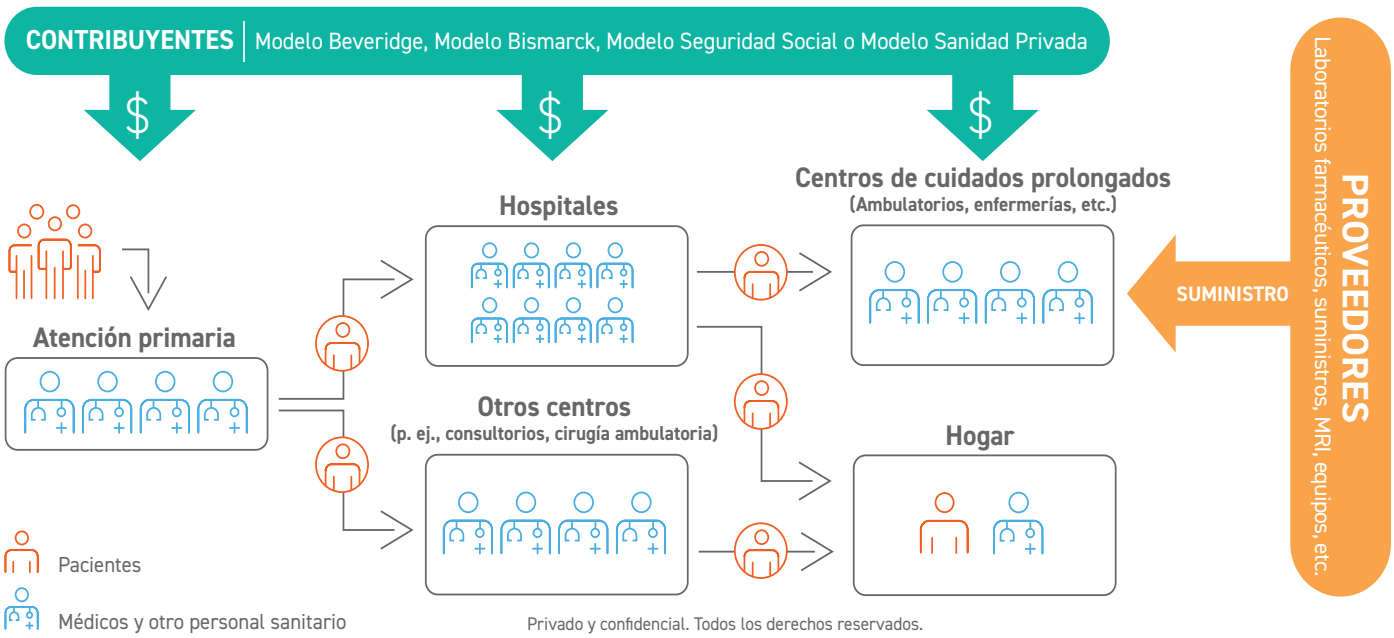
Resumen

Desde la aparición de la COVID-19, las organizaciones sanitarias o HDO (Healthcare Delivery Organizations) han ido cambiando y ampliando su consumo de recursos tecnológicos. Este crecimiento se ha producido como respuesta a la rápida aparición de la telesanidad, al influjo de los profesionales que prestan atención en remoto, a la migración a la nube de la gestión de datos y las operaciones comerciales y a la proliferación de dispositivos de telemedicina conectados. Aunque ha permitido a los profesionales proporcionar desde cualquier parte una atención de calidad, ya fuera en persona, virtual o a domicilio, también ha creado —o exacerbado— diversos retos para la ciberseguridad. Este informe examina esos retos y la complejidad de la ciberseguridad sanitaria, inherentes a esa transformación y que están generalizados en el sector sanitario global.

Introducción

Con las nuevas tecnologías y aplicaciones médicas que afectan al bienestar y la seguridad de los pacientes, en todo el ciclo de cuidados integrales, en el sector sanitario hay mucho en juego.

Los efectos en cascada de los ciberataques sobre infraestructuras sanitarias cruciales y los registros médicos electrónicos (EHR) pueden afectar a la atención de los pacientes de formas preocupantes:



- Cuando los prestadores sanitarios se quedan sin conexión por el ransomware o un ataque DDoS, los pacientes no reciben la atención necesaria.
- Los cirujanos posponen las operaciones porque la información que necesitan para realizar una intervención de vida o muerte ya no está accesible.
- El tratamiento médico se retrasa por errores en los procedimientos diagnósticos y los análisis de laboratorio.
- Los servicios de urgencias que quedan inutilizados hacen que las ambulancias tengan que desviarse a instalaciones sanitarias más alejadas, lo que puede desencadenar resultados perjudiciales e irreversibles.

La PHI es más valiosa en la Web Oscura

Los hospitales y otros prestadores sanitarios siguen siendo algunos de los objetivos más buscados por los cibercriminales internos y externos, ya que la información médica protegida (PHI) está muy demandada en la Web Oscura. Como resultado, la PHI se suele vender a precios más altos que otros tipos de información personal identificable (PII).

Por ejemplo, los números de tarjetas de crédito se desactivan y sustituyen en cuanto se detectan cargos sospechosos, lo que hace bajar su valor en el mercado. Por el contrario, los registros médicos tienen una valoración más alta porque son conjuntos de datos que no cambian y que no se pueden modificar o borrar fácilmente. Por tanto, los ciberdelincuentes pueden sacar un beneficio continuo de ellos, mientras que los pacientes afectados sufren económica y emocionalmente y tienen que dedicar su tiempo a subsanar el perjuicio resultante de esas actividades fraudulentas. Algunos ejemplos de esas actividades son la compra de medicamentos recetados, la obtención de tratamientos, la presentación de certificados médicos falsos o la obtención de préstamos personales o tarjetas de crédito utilizando los historiales robados.

Los problemas por ransomware persisten

Los delincuentes siguen buscando la forma de explotar las debilidades que los centros operativos de seguridad (SOC) del sector sanitario no han abordado o advertido, ya que las estrategias avanzadas de los hackers siguen por delante de la inversión para reforzar los controles de seguridad. Por ejemplo, los ciberdelincuentes buscan activamente las vulnerabilidades que no están actualizadas —por ejemplo, Log4j— como principales vectores para lanzar sus ataques de ransomware. Como resultado, el ransomware se considera la amenaza más significativa para el sector sanitario.

Esta tendencia probablemente continuará a lo largo de 2022, ya que el 42 %[1] de las HDO han sufrido ataques de ransomware en los últimos dos años. Además, alrededor de un 36 %[2] de esos incidentes han sucedido a través de terceros, como fue el conocidísimo caso de los ataques a la cadena de suministro en un vital software de gestión de infraestructuras que era vulnerable.

SONICWALL®

Las vulnerabilidades en el servidor de red, detrás de la mayoría de los incidentes de filtración de datos

2021 fue el peor año para el sector en cuanto a filtraciones de datos, ya que hubo un número récord de filtraciones de datos y de registros PHI expuestos. Por ejemplo, la OCR (Office for Civil Rights) de los EE. UU., que depende del Departament of Health and Human Services (HSS) informó de que más de 700 entidades asociadas (figura 1) sufrieron filtraciones que resultaron en pérdida, robo o divulgación de más de 42 millones de registros PHI personales (figura 2). Los incidentes[3] recientemente conocidos revelan que las filtraciones y vulnerabilidades suponen un comienzo aleccionador para 2022 (figura 3).

Figura 1
Filtraciones de datos en sanidad con 500 o más registros

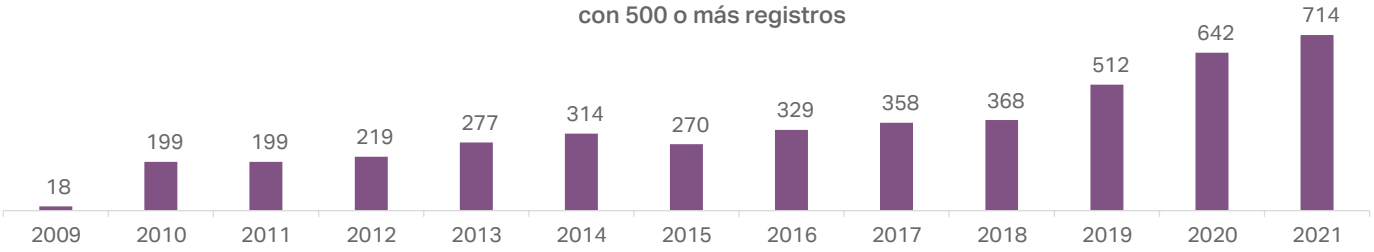
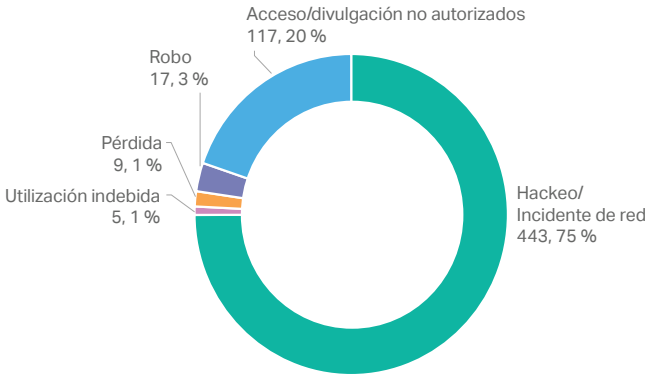


Figura 2

U.S. Department of Health and Human Services Office for Civil Rights, filtraciones de datos informadas en 2021
Total: 5



U.S. Department of Health and Human Services Office for Civil Rights, personas afectadas en 2021

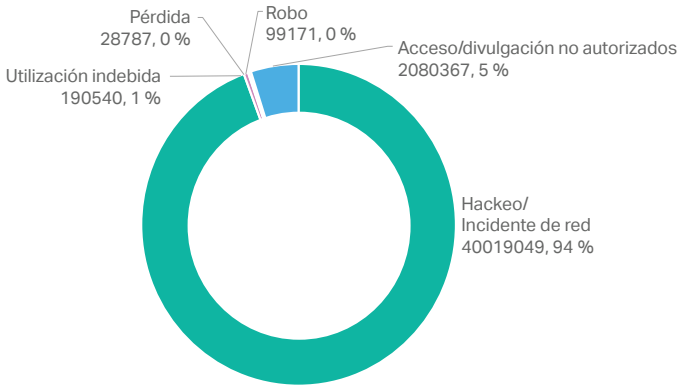
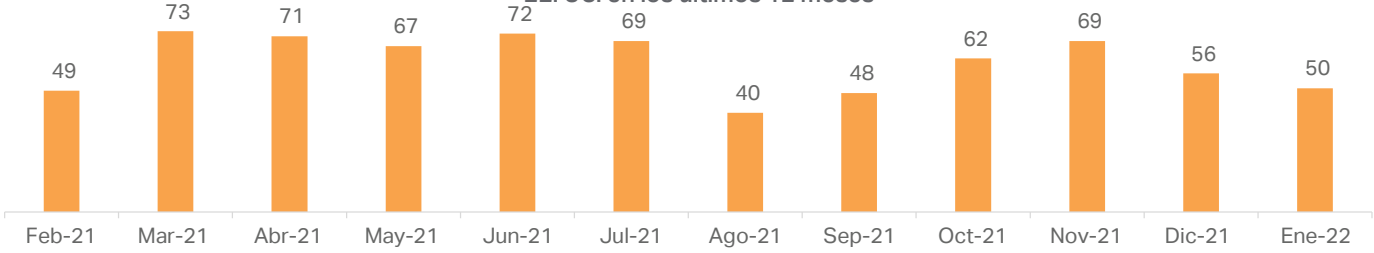
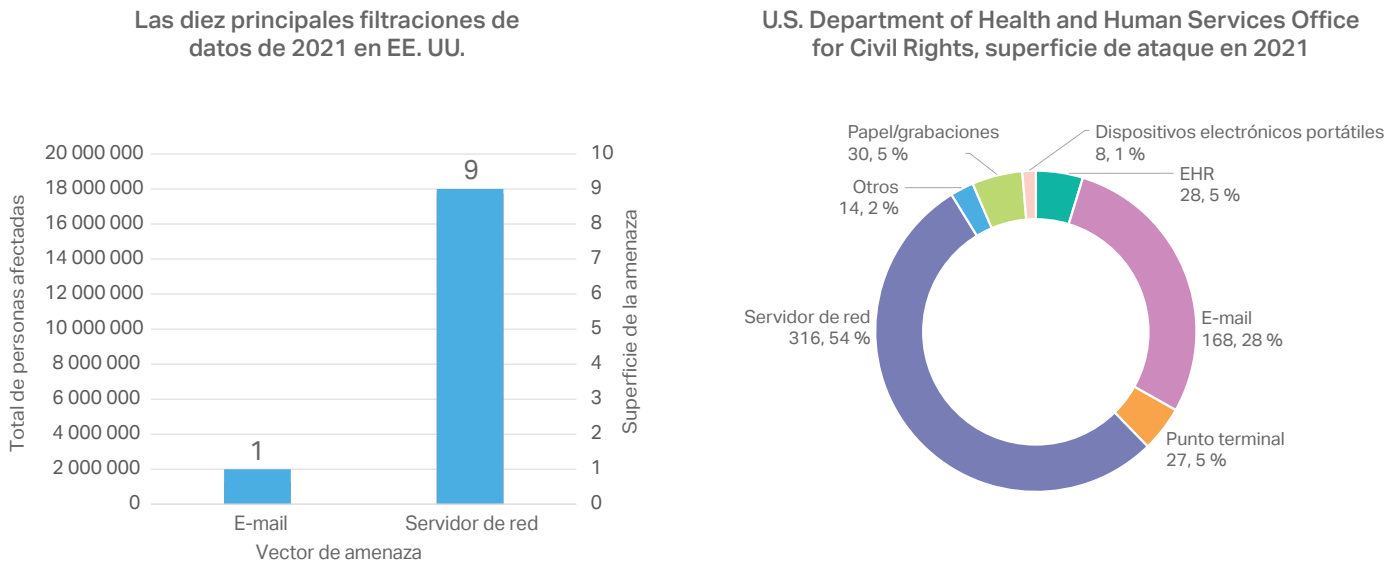


Figura 3
Filtraciones de datos sanitarios en EE. UU. en los últimos 12 meses



Las diez principales filtraciones de datos conocidas de 2021 se atribuyeron al éxito de los hackers, con la gravedad medida según el número de personas afectadas. El noventa por ciento de esas filtraciones sucedió en los servidores de red del proveedor (figura 4). Además, el servidor de red y el correo en conjunto representaron el 80 % de los vectores de ataque e impactaron negativamente en los tratamientos urgentes, lo que podría ser muy perjudicial.

Figura 4



Cuatro riesgos de ciberseguridad críticos que amenazan al sector sanitario

A pesar de las muchas ventajas que las tecnologías proporcionan a la sanidad, la adopción de nuevos dispositivos para uso médico y la interconexión entre distintos sistemas sanitarios añaden muchos riesgos. Las organizaciones sanitarias se enfrentan a cuatro desafíos significativos de seguridad, comunes a todo el sector:

1. Mantener la infraestructura crítica cubierta y siempre disponible.
2. Proteger la privacidad de los pacientes frente a los riesgos internos.
3. Preservar la integridad de los datos sanitarios.
4. Evitar filtraciones de datos por ataques de ransomware y phishing.

La ampliación de la infraestructura crítica sin invertir suficientemente en la seguridad produce una situación insostenible. Las carencias en ciberseguridad, en áreas como la gestión de parches, gestión de la configuración, controles de acceso adecuados, cifrado de datos y seguridad del portal de los pacientes, socava la misión de las HDO de proporcionar una atención de calidad y oportuna y proteger la privacidad del paciente. La protección insuficiente de los datos sanitarios que incumpla las leyes y políticas aplicables de protección de datos puede tener graves consecuencias, Algunos ejemplos: filtraciones de datos, interrupción de la atención, malos resultados de los tratamientos, interrupción de la facturación, pérdidas económicas, costes de las medidas para remediar la situación, gastos legales y por indemnizaciones, fuertes multas, pérdida de confianza, deterioro de la reputación, etc.

Conclusión

Tras más de dos años de pandemia, las organizaciones sanitarias siguen con exceso de trabajo y escasas de personal. Asimismo, la continua transformación tecnológica y digital, diseñada para mejorar la atención al paciente, aumenta la presión del personal. La solución de ciberseguridad para el sector sanitario de SonicWall está aquí para facilitar la transición y reforzar la seguridad de la infraestructura sanitaria, de forma que la atención al paciente sea más eficiente, resiliente y segura. Este stack de seguridad integrado y con gestión centralizada consta de soluciones para perímetro, centro de datos, acceso, conexión inalámbrica, correo y endpoints, lo que permite a las HDO proporcionar unos resultados sanitarios positivos para los pacientes a lo largo de todo su ciclo de atención.

Lea nuestro libro blanco «Ciberseguridad sin límites para un sector sanitario más seguro» y descubra cómo la solución de seguridad de SonicWall para el sector sanitario protege la disponibilidad de la infraestructura crítica, la integridad de los registros médicos electrónicos y la confidencialidad y privacidad de la información médica personal.

1 Fuente: Ponemom Institute: «The Impact of Ransomware on Healthcare During COVID-19 and Beyond».
2 Fuente: Ponemom Institute: «The Impact of Ransomware on Healthcare During COVID-19 and Beyond».
3 Fuente: HIPAA Journal, «January 2022 Healthcare Data Breach Report», https://www.hipaajournal.com/january-2022-healthcare-data-breach-report/

Acerca de SonicWall

SonicWall proporciona ciberseguridad sin límites, sin perímetro, para una era hiperdistribuida y una realidad laboral caracterizadas por la movilidad, el trabajo remoto y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la seguridad cibernética para hospitales, clínicas y proveedores en todo el mundo. Si desea obtener más información, visite www.sonicwall.com/healthcare.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com

ExecBrief-HealthcareCybersecurity-A4-JK-6455