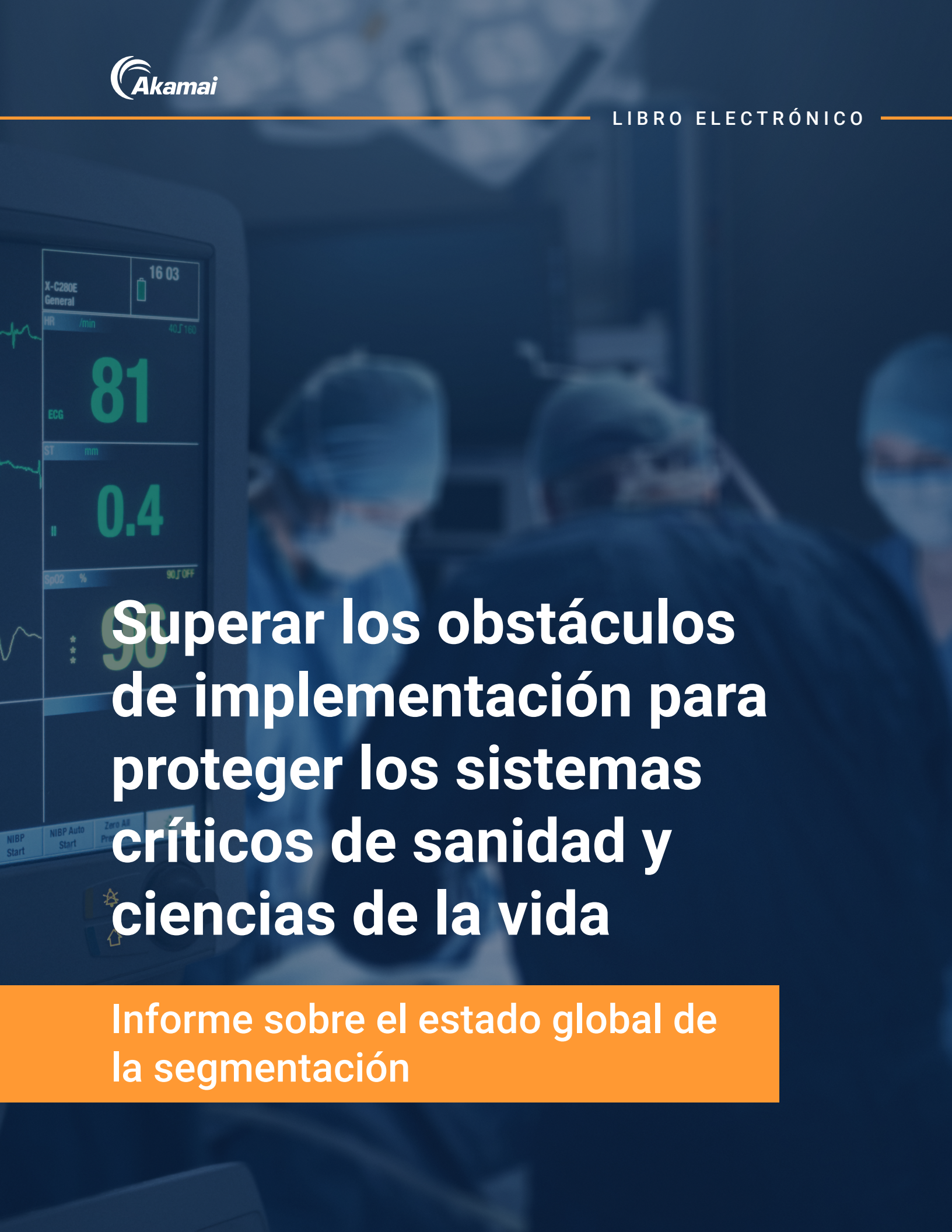
Akamai

LIBRO ELECTRÓNICO



Superar los obstáculos de implementación para proteger los sistemas críticos de sanidad y ciencias de la vida

Informe sobre el estado global de la segmentación

Tabla de contenido

Introducción

Ahora más que nunca, la TI del sector sanitario repercute en los despachos, en la sala de juntas y en la sala de exploración. Las filtraciones de datos de gran repercusión están aumentando en términos de gravedad y frecuencia, y tienen serias consecuencias para las operaciones y la reputación. Como los atacantes utilizan tácticas cada vez más sofisticadas y, en muchos casos, se alían, los peligros a los que se enfrenta el ecosistema sanitario son cada vez más frecuentes y graves. Dado el gran volumen de tecnología heredada, el valor financiero de los datos de los pacientes y los desafíos que plantea la rápida digitalización y expansión del Internet de las cosas médicas (IoMT), este entorno dinámico necesita proteger su infraestructura, su organización y sus aplicaciones y API de un modo que nadie habría imaginado hace tan solo cinco años.

Como muestran las conclusiones de este informe, los ciberataques están aumentando la presión sobre los responsables de seguridad para que elijan las soluciones adecuadas en un sector en el que el tiempo de actividad continuo es una cuestión de vida o muerte.

Los encuestados de organizaciones del sector de ciencias de la salud y de la vida de Estados Unidos, Latinoamérica, Europa, Oriente Medio, África y Asia-Pacífico coinciden de forma abrumadora en la eficacia de la segmentación a la hora de mantener protegidos los activos. No obstante, también señalan que el progreso en la implementación de la segmentación en torno a los activos y las aplicaciones empresariales esenciales no está al nivel que debería. Estos encuestados (entre los que se incluyen proveedores de atención sanitaria y expertos en tecnología sanitaria, entre otras organizaciones especializadas en servicios o productos sanitarios) afirman que el principal obstáculo al que se enfrentan las organizaciones del sector de ciencias de la salud y de la vida es la falta de experiencia a la hora de implementar la segmentación. La complejidad histórica que entraña la implementación de los métodos tradicionales de segmentación, que no cubren los dispositivos médicos, se ve agravada por el hecho de que los equipos siguen lidiando con los problemas de personal que comenzaron antes de la pandemia de COVID-19.

Una encuesta realizada por la organización sin ánimo de lucro estadounidense Healthcare Information and Management Systems Society (HIMSS) reveló que el 84 % de los expertos en TI del sector sanitario de EE. UU. tienen dificultades para contratar personal, mientras que el 67 % afirma que retener al personal les supone un problema. Según la HIMSS, la mayoría del personal no dispone de formación actualizada sobre las amenazas actuales y emergentes.

¿Y en qué consistiría esa formación actualizada? La segmentación ha demostrado tener un efecto transformador en la defensa para aquellas empresas que habían segmentado la mayoría de sus activos esenciales, ya que les permitió mitigar y contener el ransomware 11 horas más rápido que aquellas que solo tenían un activo segmentado. Imagine la diferencia que esas 11 horas pueden suponer para su equipo, sus pacientes y su reputación.

El progreso de la segmentación ha sido generalmente lento, pero los que han perseverado han logrado reducir enormemente su riesgo

La segmentación es buena. La microsegmentación es mejor.

La segmentación es un enfoque arquitectónico que divide una red en segmentos más pequeños con el fin de mejorar el rendimiento y la seguridad.

La microsegmentación es una técnica de seguridad que permite dividir lógicamente una red en distintos segmentos de seguridad hasta el nivel de carga de trabajo individual. De este modo, los controles de seguridad y la prestación de servicios se pueden definir para cada segmento único.

Los ataques de ransomware, al igual que sus efectos, siguen aumentando

Al comparar los datos de 2021 con los de 2023, se observa que el número de ataques de ransomware (tanto logrados como fallidos) contra organizaciones sanitarias en un periodo de 12 meses aumentó un 162 %. Entre los efectos de estos ataques encontramos desde tiempos de inactividad operativa, como la cancelación o el aplazamiento de procedimientos médicos, hasta problemas con la interacción entre medicamentos por falta de acceso a los historiales médicos, y desvíos de ambulancias a otros centros sanitarios.

Porcentaje de aumento del número de ataques de ransomware en los últimos 12 meses por sector (datos de 2021 frente a datos de 2023)

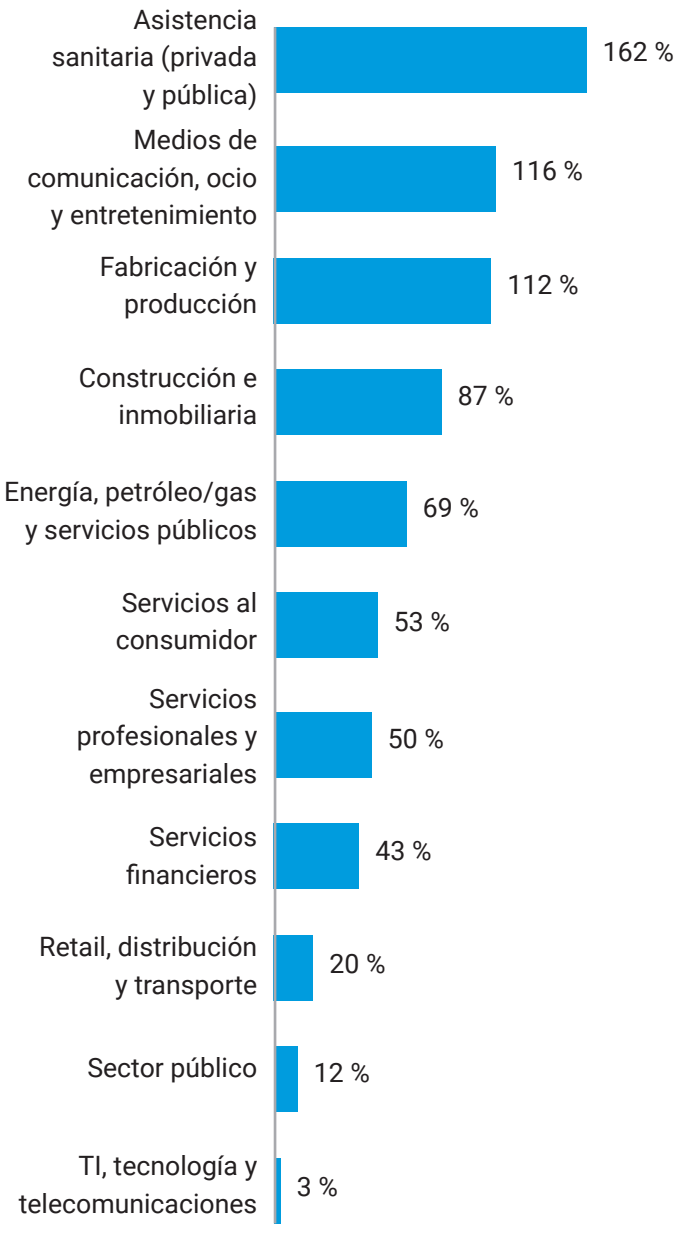


Fig. 1: ¿Cuántos ataques de ransomware se han dirigido a su organización en los últimos 12 meses (independientemente de si han tenido éxito o no)? El gráfico refleja un tamaño de base de 1200 encuestados y solo muestra el porcentaje medio de aumento del número de ataques en los últimos 12 meses, dividido por sectores.

De media, la tasa de aumento del sector sanitario es la más alta de todos los sectores. Esto podría indicar que los hackers no consideran "intocables" a las organizaciones sanitarias; ni siquiera a los hospitales infantiles, que también sufren cada vez más ataques.

Los ataques de ransomware contra organizaciones sanitarias no solo son más frecuentes en 2023 que en 2021, sino que sus repercusiones son más perjudiciales (figura 2). Los encuestados mencionan un aumento de los daños a la reputación, la pérdida de fidelidad de los clientes (pacientes) y el tiempo de inactividad de la red. Todos estos factores suben significativamente el listón para los equipos de seguridad.

Esta presión también ha repercutido en la elaboración de estrategias ágiles. El número de organizaciones sanitarias que actualizan sus estrategias o políticas de ciberseguridad al menos una vez a la semana ha aumentado del 17 % en 2021 al 25 % en 2023, no solo en respuesta al ransomware sino a una superficie de ataque en constante evolución.

Profundizando en este aspecto, estas organizaciones se encuentran entre las más propensas a sufrir pérdidas financieras tras un ataque de ciberseguridad en comparación con las de otros sectores (43 %, frente al 36 % general). También tienden más a perder la fidelidad de sus pacientes o miembros tras un ataque de ciberseguridad (48 %, frente al 33 % general). Esto demuestra que, en muchos aspectos, las organizaciones sanitarias corren mayores riesgos que otros tipos de organizaciones.

Impacto del ransomware y los ciberataques en el sector de ciencias de la salud y de la vida

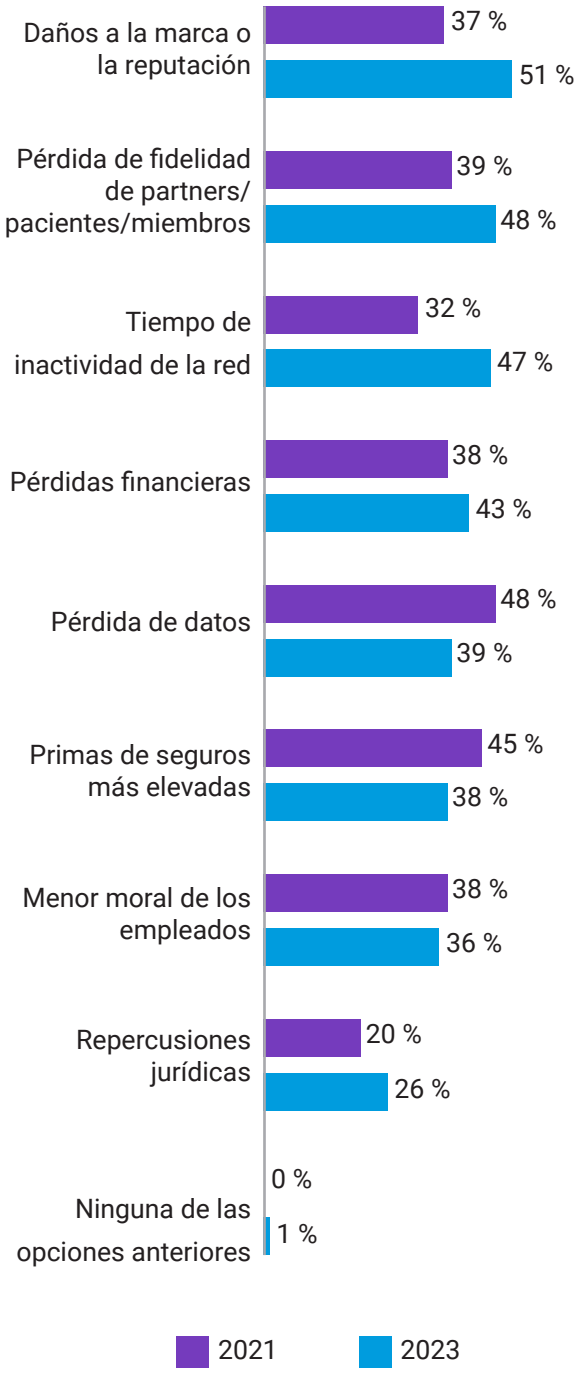


Fig. 2: En el pasado, tras detectarse ataques de ransomware u otros ciberataques, ¿cuáles de las siguientes repercusiones ha tenido en su organización? El gráfico muestra el tamaño de la base por año, sin mostrar todas las opciones de respuesta, dividido por datos históricos (2021=112, 2023=157). Solo se incluyen datos del sector sanitario.

La segmentación se considera la piedra angular de Zero Trust

Los encuestados del sector de ciencias de la salud y de la vida coinciden en que la segmentación es importante para garantizar la seguridad de sus organizaciones, sobre todo a la hora de hacer frente al malware.

Zero Trust es una estrategia de seguridad de red basada en la filosofía de que ninguna persona o dispositivo dentro o fuera de la red de una organización debe tener acceso para conectarse a sistemas de TI o cargas de trabajo a menos que se considere explícitamente necesario. En resumen, significa cero confianza implícita.

El 64 % de los encuestados afirma que la segmentación es extremadamente importante, y el 94 % considera que es fundamental para poner fin a los peores ataques.

A menudo, la adopción de Zero Trust se ve impulsada por circunstancias que escapan al control de los responsables de TI del sector sanitario. Al citar los motivos por los que su organización inició un proyecto de segmentación, un tercio (33 %) de los encuestados del sector sanitario afirma que se debió al interés de su gobierno por la ciberseguridad, y casi el mismo número (29 %) reconoce que se debió a que ya habían sido víctimas de un ataque de ransomware.

Pero, solo uno de cada tres (34 %) encuestados del sector sanitario afirma que su marco Zero Trust está totalmente completo y definido y, por tanto, maduro. Esta cifra se encuentra entre las más bajas de todos los sectores, siendo algunos sectores (como la construcción y los servicios financieros) notablemente más propensos a contar con un marco Zero Trust maduro (53 % y 47 %, respectivamente).

Es probable que la madurez de Zero Trust esté impulsada por las organizaciones sanitarias de EE. UU. (donde el 50 % afirma tener un marco totalmente completo y definido), en comparación con las demás regiones (solo el 23 % de los demás países y regiones afirma que su marco Zero Trust está totalmente completo y definido). Esto refleja la tendencia general, por la que las organizaciones estadounidenses de todos los sectores declaran haber sido víctimas de ciberataques en comparación con otras regiones (115 en los últimos 12 meses, frente a la media general de 86).

Por lo tanto, las organizaciones sanitarias se enfrentan a desafíos en lo que respecta a Zero Trust. Los encuestados de este sector tienden a tener más problemas relacionados con tecnología propia a la hora de segmentar su red (41 %, frente al 32 % general), y también tienden más a experimentar dificultades presupuestarias a la hora de implementar Zero Trust (47 %, frente a una media del 37 % en todos los sectores). El apoyo de un partner experimentado puede ayudar a superar algunos de estos obstáculos: uno de los aspectos de un marco Zero Trust que más les cuesta implementar a las organizaciones sanitarias es la carga de trabajo de las aplicaciones (68 %, frente al 60 % general). Un partner puede suplir las carencias de competencias, que señalaron el 45 % de dichas organizaciones.

La mayoría de los encuestados de organizaciones sanitarias aspiran a ir más allá e implementar la microsegmentación, que protege las cargas de trabajo de las aplicaciones a un nivel detallado:

El 92 % de los encuestados del sector sanitario afirma que la microsegmentación es, al menos, una prioridad alta, y el 43 % la considera su máxima prioridad. De todos los sectores encuestados, solo el 34 % considera la microsegmentación como su máxima prioridad, lo que demuestra que las organizaciones del sector sanitario tienden más, de media, a valorar y abogar por los marcos Zero Trust.

Las implementaciones son lentas, pero la perseverancia produce resultados transformadores

A pesar del consenso generalizado de que la segmentación es fundamental para prevenir los ciberataques, su implementación avanza despacio.

En 2023, solo el 36 % de las organizaciones del sector sanitario habían segmentado más de dos áreas de negocio críticas, y el 43 % inició por última vez un proyecto de segmentación de red hace dos o más años, lo que sugiere que las iniciativas se han estancado.

Las áreas críticas

- Aplicaciones esenciales
- Aplicaciones orientadas al público
- Controladores de dominio
- Terminales
- Servidores
- Activos/datos esenciales del negocio

La lentitud de las implementaciones se puede atribuir a muchos de los principales obstáculos a los que se enfrentan los encuestados del sector sanitario: la falta de competencias y experiencia a la hora de implementar la segmentación (45 %), el aumento de los cuellos de botella que afectan al rendimiento (como los provocados por la necesidad de solucionar manualmente los errores, 44 %) y el uso de tecnología propia (41 %, figura 3). La falta de competencias y experiencia, en particular, es un problema mayor para las organizaciones del sector sanitario que para las organizaciones de cualquier otro sector (todas por debajo del 45 % del sector sanitario, con una media transversal del 39 %). Estos resultados coinciden con los recientes hallazgos de Ponemon Institute, una de las principales organizaciones de investigación sobre seguridad de TI, sobre las amenazas predominantes en el sector sanitario, entre las que se incluyen principalmente el ransomware y los esquemas de ataque al correo empresarial (BEC). Si bien la remuneración competitiva de los profesionales de TI del sector sanitario es uno de los desafíos, el creciente volumen de requisitos normativos complejos es otro.

Las organizaciones sanitarias de todo el mundo siguen sufriendo las secuelas de la pandemia de COVID-19 y la presión que ejerció sobre el capital humano y fiduciario, lo que agrava estos desafíos.

Obstáculos detectados al segmentar la red en el sector de ciencias de la salud y de la vida

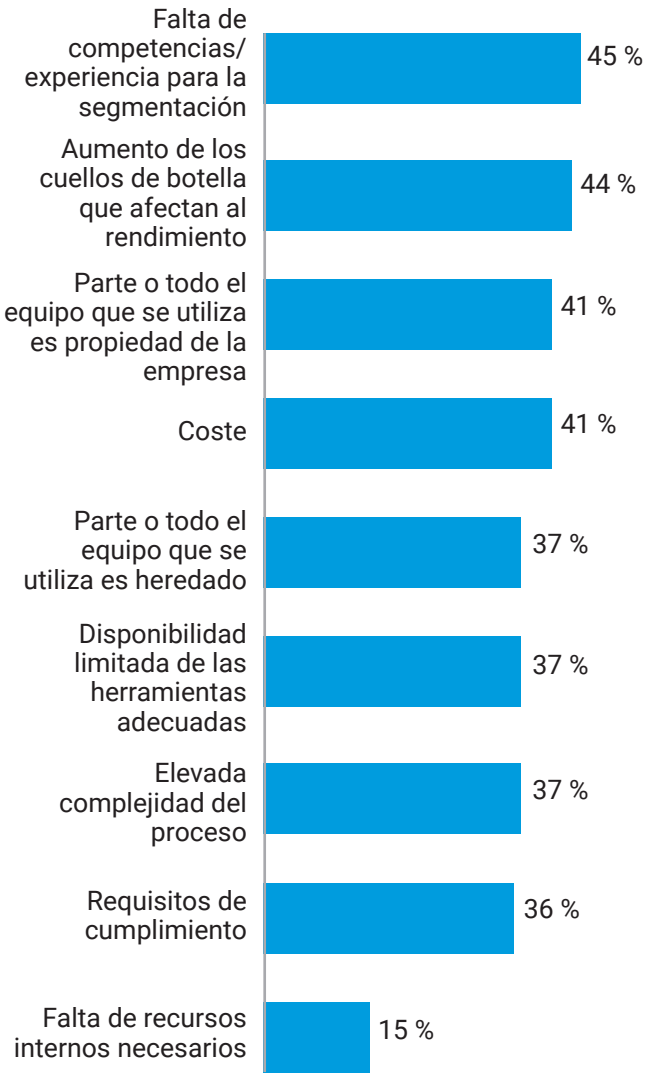


Fig. 3: Si su organización ha tenido o prevé tener problemas al segmentar la red, ¿cuáles han sido o cree que serán? El gráfico muestra un tamaño de base de 157 en 2023 y no se muestran todas las opciones de respuesta.
Esta pregunta solo se mostró a los encuestados de organizaciones que han segmentado su red en algún momento, y solo se incluyen datos del sector sanitario.

A pesar del lento avance, las tasas de segmentación están aumentando gradualmente en todos los sectores. Dentro del sector sanitario, el porcentaje de organizaciones con aplicaciones o datos empresariales esenciales segmentados aumentó un 20 % y el de servidores segmentados un 18 % entre 2021 y 2023. Pero, aunque estos aumentos superan la media general observada en todos los sectores (12 y 8 %, respectivamente), las principales vulnerabilidades exigen una aceleración de las tasas de segmentación. El sector sanitario es el que más probabilidades tiene de que un empleado o usuario sea el motivo o el origen de que un atacante obtenga acceso a la red (47 %, frente al 26 % general). Esta cifra duplica con creces la de otros sectores en los que el cumplimiento normativo también es fundamental, como los servicios financieros y el sector energético (ambos con un 19 %). El impacto de este tipo de ataques se puede minimizar con la segmentación y, teniendo en cuenta la importancia que tienen numerosos sistemas en las organizaciones sanitarias (y que hay vidas en juego), resulta evidente que es necesario implementar la segmentación lo antes posible.

Conclusiones extraídas de la segmentación de seis áreas de negocio críticas

Al mejorar la visibilidad se reduce el riesgo, algo fundamental en un sector reacio al riesgo. Cuantos más activos se protejan y segmenten, más seguras estarán las organizaciones sanitarias, lo que permitirá a los equipos de seguridad detectar más rápidamente las amenazas y responder de forma mucho más eficaz.

Los hallazgos de Vanson Bourne muestran que, tras una filtración, la recuperación se produce 11 horas más rápido con la segmentación. Hablemos de cifras: en las organizaciones sanitarias que han implementado la segmentación en las seis áreas críticas, se tarda una media de 3 horas en detener por completo un ataque de ransomware; en las que solo tienen segmentado un activo, se tarda una media 14 horas.

Del mismo modo, la segmentación permite contener el movimiento lateral 11 horas más rápido.
En aquellas organizaciones que han implementado la segmentación en seis áreas críticas, se tarda una media de tres horas en limitar significativamente el movimiento lateral de un ataque de ransomware. En aquellas con segmentación en un solo activo, se tarda una media de 14 horas.

Piense en la diferencia que supondrían esas 11 horas para su equipo, el daño a la marca y los costes incurridos en cualquiera de las situaciones.

Para detener un ataque
3 horas

El tiempo que se tarda, de media, en detener por completo un ataque de ransomware en aquellas organizaciones que han segmentado los seis activos empresariales. En aquellas que solo han segmentado un activo: **14 horas**

Para limitar el movimiento
3 horas

El tiempo que se tarda, de media, en limitar significativamente el movimiento lateral de un ataque de ransomware en aquellas organizaciones que han segmentado los seis activos empresariales. Para aquellos que solo han segmentado un activo: **14 horas**

Cómo una solución de microsegmentación basada en software ayuda a resolver los desafíos

La microsegmentación no solo permite una segmentación más avanzada y detallada, sino que también es más fácil de implementar.

Las soluciones basadas en software, como Akamai Guardicore Segmentation, se pueden implementar rápidamente sin tener que realizar cambios físicos en la red. No es necesario volver a asignar la dirección IP a los nuevos segmentos ni preocuparse por dónde se encuentran físicamente los servidores y los dispositivos. Esto hace que la solución sea mucho más rápida y fácil de implementar que los enfoques basados en la infraestructura, como los firewalls y las VLAN. Y, como la solución no depende del sistema operativo subyacente para la aplicación de las políticas, funciona a la perfección en todos los equipos y sistemas operativos: desde servidores bare metal hasta implementaciones multinube, desde tecnología heredada como Windows Server 2003 hasta los últimos dispositivos del Internet de las cosas médicas (IoMT) y tecnología contenedorizada. Esto significa que solo necesita gestionar una única solución con una interfaz para visualizar y controlar las conexiones realizadas por diferentes sistemas operativos y dispositivos en todo el entorno, independientemente de su ubicación física.

Cómo facilita la implementación

Akamai Guardicore Segmentation genera primero una imagen interactiva de todas las conexiones que se realizan en su entorno, lo cual es un componente fundamental para superar los principales obstáculos de la implementación. Además, Akamai ha incorporado en su solución formas activas de superar los cuellos de botella que afectan al rendimiento y los requisitos de cumplimiento.

Los cuellos de botella que afectan al rendimiento no surgen necesariamente de una tensión técnica en el sistema provocada por una solución de segmentación, sino de los cuellos de botella derivados de la plantilla. El tiempo y el esfuerzo que supone tener que segmentar manualmente las áreas de negocio y, a continuación, solucionar manualmente los problemas de esas áreas cuando las cosas no funcionan puede ser tremendo. Akamai trabaja para resolver este problema (y el principal obstáculo para la implementación: la falta de experiencia) reduciendo el tiempo dedicado a la segmentación manual y ofreciendo asistencia técnica y servicios profesionales de primer nivel. Nuestros expertos en segmentación colaboran con usted durante todo el proceso de implementación para garantizar el cumplimiento de sus objetivos de segmentación en su exclusivo entorno de TI.

La asistencia para la implementación también proviene de la propia solución: sus recomendaciones de políticas y etiquetado basadas en IA y sus plantillas de políticas listas para usar para casos de uso comunes ahorran tiempo y clics, simplifican el flujo de trabajo, reducen el tiempo total de implementación de políticas y evitan configuraciones erróneas debido a errores humanos. Para uno de sus clientes, Akamai desarrolló un proyecto de segmentación detallada con una duración estimada de dos años y un coste total de más de 1 millón de dólares estadounidenses. Akamai consiguió completarlo en tan solo seis semanas con un solo ingeniero, lo que redujo el coste total del proyecto en un 85 %, y demostró que la segmentación detallada se puede implementar de forma rápida y sencilla, sin sufrir cuellos de botella.

Cómo facilita el cumplimiento

Numerosas organizaciones del sector de ciencias de la salud y de la vida implementan Akamai Guardicore Segmentation para garantizar el cumplimiento de una serie de normativas nacionales e internacionales, como HIPAA, RGPD, PCI DSS y muchas más. Estos requisitos normativos suelen exigir que los datos dentro del ámbito de aplicación se separen de otros sistemas de su entorno. Aunque hacer esto puede resultar extremadamente difícil si se utilizan firewalls y VLAN, nuestra solución basada en software le permite crear segmentos específicamente para los datos dentro del ámbito de aplicación y aplicar reglas de comunicación sobre lo que puede y no puede acceder a esos datos. Con nuestro mapa visual con vistas casi en tiempo real y con perspectiva histórica, puede certificar que cumple estos requisitos mostrando físicamente que los usuarios y equipos no autorizados no están accediendo a los datos dentro del ámbito de aplicación.

Persevere con la solución y la asistencia adecuadas para transformar su estrategia de seguridad

La segmentación puede ser extremadamente difícil de implementar. Pero, como muestra este informe, quienes logran implementarla de forma eficaz ven reducciones masivas en su riesgo cibernético. Disponer de una segmentación adecuada limita el movimiento lateral de las amenazas y le permite reaccionar más rápido durante una filtración. Y después de una filtración, las tareas de recuperación están protegidas y tardan menos tiempo en completarse.

La elección de una solución diseñada para superar los desafíos comunes de la implementación de la segmentación, y la colaboración con expertos que están a su disposición a medida que avanza en el proceso, le sitúa en la mejor posición posible para transformar su estrategia de seguridad. Además, cuantas más áreas de negocio segmente, más avanzará también en su arquitectura Zero Trust, ya que reducirá su riesgo actual y garantizará una defensa de primera línea contra futuros vectores de amenazas.

Conclusiones

Los ciberatacantes se dirigen cada vez más a las organizaciones del sector sanitario: los ataques de ransomware contra organizaciones sanitarias aumentaron un 162 % entre 2021 y 2023. En comparación, el sector energético sufrió un 69 % más de ataques en ese periodo de tiempo, y el de los servicios financieros un 43 %.

Los encuestados del sector sanitario tienden a decir que su organización sufrió pérdidas económicas tras un ataque de ciberseguridad: el 43 % lo afirma, frente al 36 % de los encuestados de todos los sectores.

La segmentación y la microsegmentación son más importantes en el sector sanitario que en muchos otros sectores: los responsables de la toma de decisiones de seguridad de TI del sector sanitario (64 %) son más propensos a afirmar que la segmentación de red es extremadamente importante para garantizar la seguridad de sus organizaciones que los de muchos otros sectores, como la construcción (58 %), la fabricación (53 %) y el e-commerce (48 %). La opinión de los responsables de la toma de decisiones de seguridad de TI en el sector sanitario coincide con las cifras de los encuestados en organizaciones de servicios financieros y del sector energético (ambos con un 66 %).

Las organizaciones sanitarias tienden a tener un menor nivel de madurez en lo que respecta a la implementación de su marco de seguridad Zero Trust: las empresas del sector sanitario no tienden a afirmar que su implementación de Zero Trust está totalmente completa y definida (34 %), a diferencia de las del sector de los servicios financieros (47 %), el sector energético (46 %) y el sector del e-commerce (42 %).

Nuestro grupo de estudio

En el estudio de investigación completo, entrevistamos a 1200 responsables de la toma de decisiones de TI y seguridad de 10 países para medir el progreso que las organizaciones han realizado en la protección de sus entornos, haciendo hincapié en el papel que desempeña la segmentación.

Se les hicieron preguntas sobre sus enfoques de seguridad de TI y sus estrategias de segmentación, así como sobre las amenazas a las que se habían enfrentado sus organizaciones en 2023. Estos datos y resultados nos ofrecen detalles sobre cómo han cambiado las estrategias de seguridad desde 2021 y en dónde se tienen que realizar mejoras todavía.

Se encuestó a personas de países de todo el mundo, como Estados Unidos, India, México, Brasil, Reino Unido, Francia, Alemania, China, Japón y Australia. Procedían de organizaciones con más de 1000 empleados, así como de una amplia gama de sectores y subsectores.

Nota: Esta muestra difería ligeramente de la de 2021. Tamaño de las muestras: 2023: 1200 encuestados; 2021: 1000 encuestados. En 2023, también se entrevistó a personas procedentes de Australia, Japón y China. Los sectores diferían ligeramente de los de 2021. En 2023, nos centramos específicamente en el e-commerce como sector por derecho propio.

Para elaborar este informe sobre el sector de ciencias de la salud y de la vida, analizamos las respuestas de 157 (2023) y 112 (2021) participantes que trabajan en el sector.
Estos encuestados representan a los mismos países que el informe principal (EE. UU., India, México, Brasil, Reino Unido, Francia, Alemania, China, Japón y Australia).

El estudio de investigación completo incluía los siguientes sectores adicionales: e-commerce (190), servicios financieros (173), TI, tecnología y telecomunicaciones (125), energía, petróleo/gas y servicios públicos (94), fabricación y producción (91), retail, distribución y transporte (81), medios de comunicación, ocio y entretenimiento (63), construcción e inmobiliaria (60), servicios profesionales y empresariales (58), sector público (46), servicios al consumidor (33) y otros sectores (29).

Obtenga más información sobre Akamai Guardicore Segmentation

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. Puede obtener más información sobre las soluciones de Akamai para el sector de ciencias de la salud y de la vida en akamai.com/healthcare y www.akamai.com/blog. También puede seguir a Akamai Technologies en X, anteriormente conocido como Twitter, y en LinkedIn. Publicado el 24 de mayo.

Vanson Bourne es una empresa independiente especializada en investigaciones de mercado para el sector tecnológico. La reputación de solidez y credibilidad de sus análisis se basa en principios de investigación rigurosos y en su capacidad para recabar las opiniones de los responsables de la toma de decisiones sénior en los diferentes cargos técnicos y comerciales, en todos los sectores de actividad y en los principales mercados. Para obtener más información, visite www.vansonbourne.com.