WHITE PAPER

Patrocinado por: Neosecure

Los servicios de seguridad gestionados son la mejor manera de enfrentar los principales desafíos para implementar la ciberseguridad: equipos normalmente reducidos, amenazas en constante evolución y las complejidades para administrar y configurar.

Estado de adopción de los servicios de seguridad gestionados en América Latina

Abril, 2023

Escrito por: Luiz Monteiro, Analista Senior de Mercado de Servicios.

I. Preocupaciones sobre la seguridad en las organizaciones

Las empresas viven en una realidad en la que los ataques exitosos dan lugar a una amplia cobertura y divulgación. Sin embargo, a pesar de que están presentes en las organizaciones, los equipos de seguridad suelen ser de tamaño reducido, independientemente del tamaño, la vertical o la ubicación de la empresa. Según el estudio de *IDC Brasil, Adoção de Serviços Gerenciados de Segurança, 2023* desarrollado por IDC en octubre de 2023, con una muestra de 286 empresas encuestadas en Argentina, Brasil, Chile, Colombia, Perú y México, el promedio de LATAM es de 3 recursos dedicados a la seguridad en empresas de 500 a 999 empleados, 7 recursos en empresas de 1.000 a 1.999, 13 recursos en empresas de 2.000 a 4.999 y 26 en empresas de más de 5.000 empleados. Se trata de una proporción baja, sobre todo si se tiene en cuenta que a estas muestras se suma la cantidad de recursos dedicados a la seguridad, ya sean propios o contratados por terceros.

En otra encuesta realizada por IDC Brasil, *IDC Cibersecurity Report Brazil 2023*, que se dirigió a un universo de tomadores de decisión de 120 empresas con más de 50 empleados en todas las verticales y estados del país, los ejecutivos señalan la necesidad de mantener la seguridad y confiabilidad de todos los activos digitales, pero demuestran un alto grado de preocupación por el posible daño a la imagen de la organización en caso de eventos de seguridad (4,75 en una escala de 1 a 5). Prácticamente, con la misma puntuación que el segundo ítem (4,74 en una escala de 1 a 5), los encuestados manifiestan una alta preocupación por la posibilidad de fuga o pérdida de datos de manera involuntaria por parte de empleados y socios, como se muestra en la Figura 1.

EN UNA MIRADA

ASPECTOS IMPORTANTES

- La seguridad sigue siendo una de las principales iniciativas en toda la región de LATAM, y es una prioridad para los ejecutivos de TI en organizaciones de todos los tamaños, verticales o ubicaciones geográficas.
- En general, 44% de las organizaciones en LATAM tienen menos de 25 empleados en las áreas de TI, y 46% tienen menos de 5 empleados enfocados a la Seguridad, en un escenario de equipos de seguridad reducidos, independientemente del tamaño o vertical de las empresas.
- 77% de las organizaciones han contratado o ya tenían contratos en curso con proveedores de servicios de seguridad gestionados para apoyarlas en sus demandas de seguridad de la información.
- En Brasil, las organizaciones tienden a trabajar con un mayor número de socios de Servicios de Seguridad (hasta 7), lo que aumenta la complejidad en su gestión, lo que requiere la búsqueda de socios que cuenten con equipos con alta experiencia y capacidad para comprender y abordar cualquier problema de seguridad.

FIGURA 1: **Las principales preocupaciones de la organización sobre la ciberseguridad**

Escala de 1 a 5, donde 1 es no importante y 5 es muy importante.

Fuente: IDC Cybersecurity Report Brazil 2023.

Además, el uso de múltiples entornos y tipos de infraestructura en la búsqueda de eficiencia, rapidez y fluidez en las operaciones también ha sumado complejidades que antes no existían para los gestores de la seguridad de la información en las organizaciones. Este contexto ha hecho que acercarse a los proveedores de Servicios de Seguridad Gestionados[1] sea algo natural y necesario para las empresas, que a su vez se preparan cada vez más, según sus respectivos momentos, madurez y avance en las disciplinas necesarias para entender y recorrer el camino que conducen a la ciberresiliencia.

En este documento presentaremos el estado de la Adopción de los Servicios de Seguridad Gestionados en América Latina, con base en las respuestas de los 286 ejecutivos en una encuesta realizada por IDC, las consideraciones y los beneficios de contar con servicios profesionales y administrados para enfrentar los desafíos intrínsecos a la implementación de la principal iniciativa de Tecnología de la Información (TI) para satisfacer las necesidades de las organizaciones.

II. Estado de madurez de la seguridad en LATAM

Actualmente, 53% de las organizaciones en América Latina consideran que tienen una estrategia de seguridad definida e implementada, mientras que 27% (Figura 2) consideran que su estrategia está definida y en fase de implementación. Esto indica que existe una autopercepción bastante positiva sobre sus posiciones en lo que respecta a la seguridad.

[1] Los Servicios de Seguridad Gestionados (Managed Security Services MSS) son servicios de ciberseguridad para dispositivos y redes públicos y privados que son operados por proveedores externos (normalmente en un modelo basado en el consumo) e incluyen seguridad como firewalls y detección y análisis oportunos de intrusiones reales.

FIGURA 2: **Percepción organizacional sobre sus estrategias de seguridad**

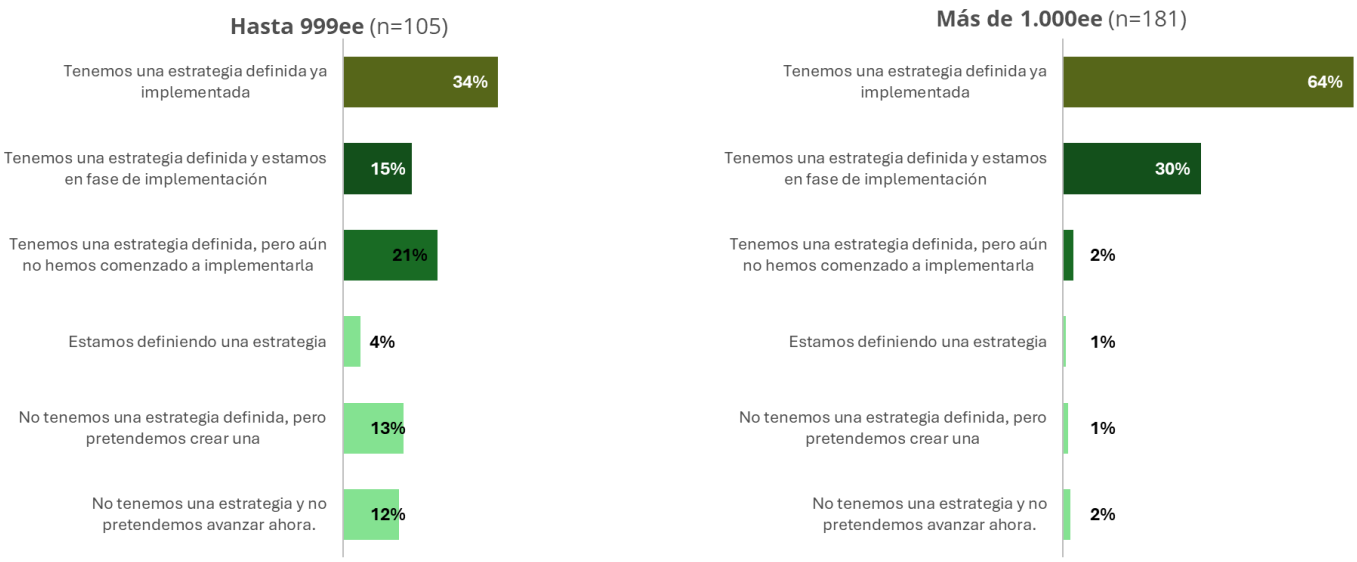
	LATAM	Comercio	Finanzas	Salud	Manufactura	Servicios	Telecomunicaiones y medios	Otros
Tenemos una estrategia definida ya implementada	53%	54%	54%	45%	57%	62%	47%	53%
Tenemos una estrategia definida y estamos en la fase de implementación	27%	27%	21%	29%	27%	21%	39%	26%
Tenemos una estrategia definida, pero todavía no la implementamos	7%	8%	8%	2%	8%	7%	3%	13%
Estamos definiendo una estrategia	2%	2%	5%	0%	0%	2%	0%	3%
No tenemos una estrategia definida, pero pensamos crearla	6%	2%	5%	14%	5%	5%	6%	3%
No tenemos una estrategia y no pretendemos avanzar en eso ahora	6%	8%	8%	10%	3%	2%	6%	3%

Fuente: IDC Brasil, Adoção de Serviços Gerenciados de Segurança, 2023. n= 286 de la Figura 2 muestran cifras redondeadas.

Sin embargo, al considerar el tamaño de las organizaciones (Figura 3), la postura se percibe de manera diferente: las organizaciones con más de 1.000 empleados se reconocen con una postura más desarrollada (94% con estrategias ya implementadas o en implementación) versus una postura diferente de las empresas más pequeñas, donde menos de la mitad, el 49%, parecen tener estrategias implementadas o en proceso de implementación. Considerando el total de la muestra encuestada, el 20% de las organizaciones aún no han implementado sus estrategias de seguridad, una parte importante de las empresas si consideramos la firmografía[2] de las organizaciones de la región, predominantemente pequeñas o medianas (Pymes).

[2] *Firmografía- es una manera de segmentar a las empresas con base em atributos semejantes (número de empleados, por facturación, entre otros).*

FIGURA 3: **Percepción organizacional sobre sus estrategias de Seguridad, por tamaño de la organización**

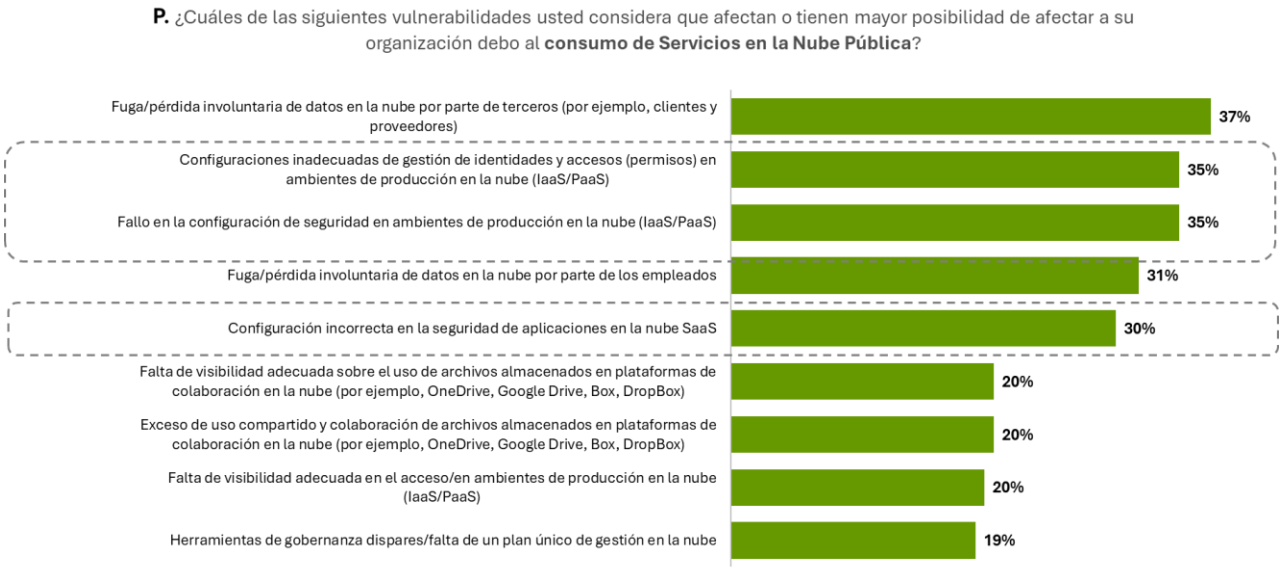


Fuente: IDC Brasil, Adoção de Serviços Gerenciados de Segurança, 2023.

Desde el punto de vista de las industrias, las organizaciones de Servicios, Retail, Manufactura y Finanzas muestran una madurez por encima del promedio latinoamericano (que es de 53%) y ya cuentan con una estrategia definida e implementada. Por país, las organizaciones de Brasil (65%) y México (58%) son más maduras que las de Argentina, Chile, Colombia y Perú. Pero esto también puede estar asociado con el tamaño de los propios equipos de TI y seguridad: normalmente, el promedio de empleados en los equipos de TI en empresas de hasta 999 empleados es de 15, mientras que el equipo de seguridad suele tener tres recursos. Las empresas de 1.000 a 1.999 empleados tienen un promedio de 27 empleados en TI y siete en seguridad. Las empresas de entre 2.000 y 4.000 empleados cuentan con un promedio de 51 recursos de TI y 13 dedicados a la seguridad. El último grupo, de empresas con más de 5.000 empleados, suele tener 97 empleados en TI y 26 centrados en la seguridad de la información. También es destacable que, en general, 44% de las organizaciones en LATAM tienen menos de 25 empleados en las áreas de TI y 46% tienen menos de cinco empleados enfocados en la Seguridad, en un escenario que muestra equipos de seguridad reducidos, independientemente del tamaño o vertical de las empresas.

Este panorama es preocupante, si sumamos a la ecuación la adopción de la nube en los negocios digitales, donde las vulnerabilidades más críticas asociadas a la nube pública están vinculadas a cuestiones técnicas sobre el acceso y uso de las plataformas (Figura 4): gestión de identidades y accesos en ambientes de producción en la nube y configuración de seguridad en la nube (IaaS, PaaS), así como la configuración de seguridad de las aplicaciones SaaS, son ítems en los que las organizaciones deben apoyarse en un socio de Servicios de Seguridad Gestionados con mejores prácticas, personal actualizado y cualificado.

FIGURA 4: **Vulnerabilidades que más pueden afectar a las organizaciones debido al consumo de servicios de nube pública**



Fuente: IDC Brasil, Adoção de Serviços Gerenciados de Segurança, 2023.

III. Razones por las que se contratan los Servicios de Seguridad Gestionados

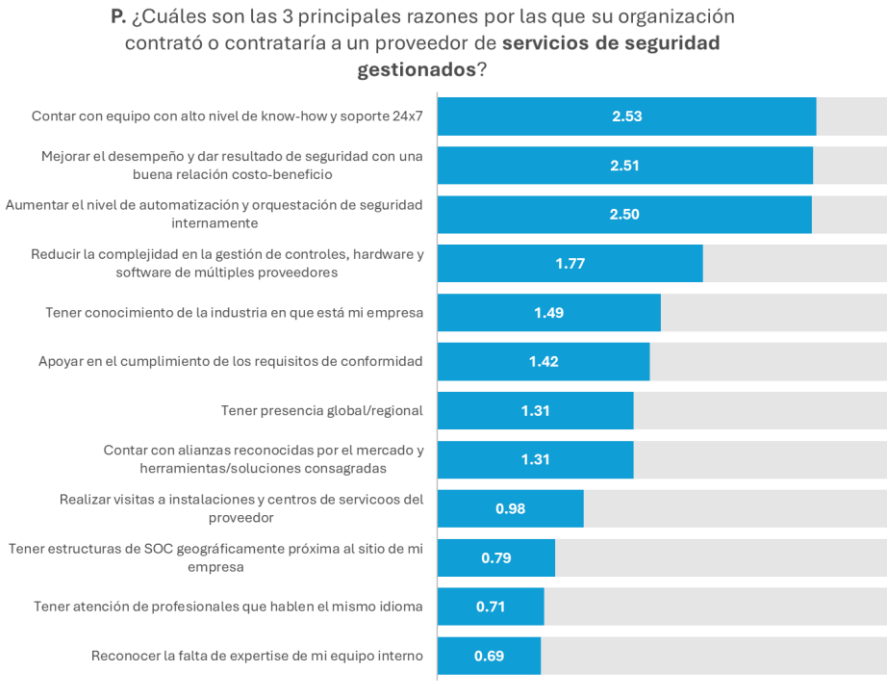
En América Latina, las inversiones corporativas (Business-to-Business) en soluciones de Seguridad alcanzaron los 7.288[3] millones de dólares en 2023; 53,3% corresponde a Servicios; 5,9% a Software y el 10,8% a Hardware. De acuerdo con los pronósticos de IDC, los servicios de seguridad profesionales y gestionados crecerán a una tasa de crecimiento anual compuesta (CAGR) del 12,2% entre 2023 y 2027[4], lo que refleja una tendencia creciente en su adopción en la región.

Esta información se ve reforzada por el estudio de *IDC Brasil, Adoção de Serviços Gerenciados de Segurança, 2023,* en el que 77% de las organizaciones han contratado o ya tenían contratos vigentes con proveedores de Servicios de Seguridad Gestionados para apoyarlas en sus demandas relacionadas con la seguridad de la información. Solo una minoría de 14% dijo que no tiene proveedores de servicios de seguridad gestionados, eligiendo trabajar solo con equipos internos en este contexto.

Para entender qué impulsa la adopción de estos servicios, las organizaciones señalan principalmente el hecho de que pueden contar con equipos con alto know-how y soporte continuo, de 24x7x365 (con una puntuación de 2,53 en una escala de 1 a 3). Las principales razones también apuntan al mejor rendimiento de las soluciones en el ambiente empresarial con un buen costo-beneficio, además de la búsqueda de una mayor automatización y orquestación. Este factor nos indica el tipo de actuación esperada de los servicios gerenciados en las empresas.

[3] Fuente: IDC Worldwide Security Spending Guide, Jul/2023.
[4] Fuente: IDC Worldwide Security Spending Guide, Jul/2023 I Professional Services consideram consultoria, integração e suporte.

FIGURA 5: **Principais razones para contratar un proveedor de servicios de seguridad gestionados**



Fuente: IDC Brasil, Adoção de Serviços Gerenciados de Segurança, 2023.

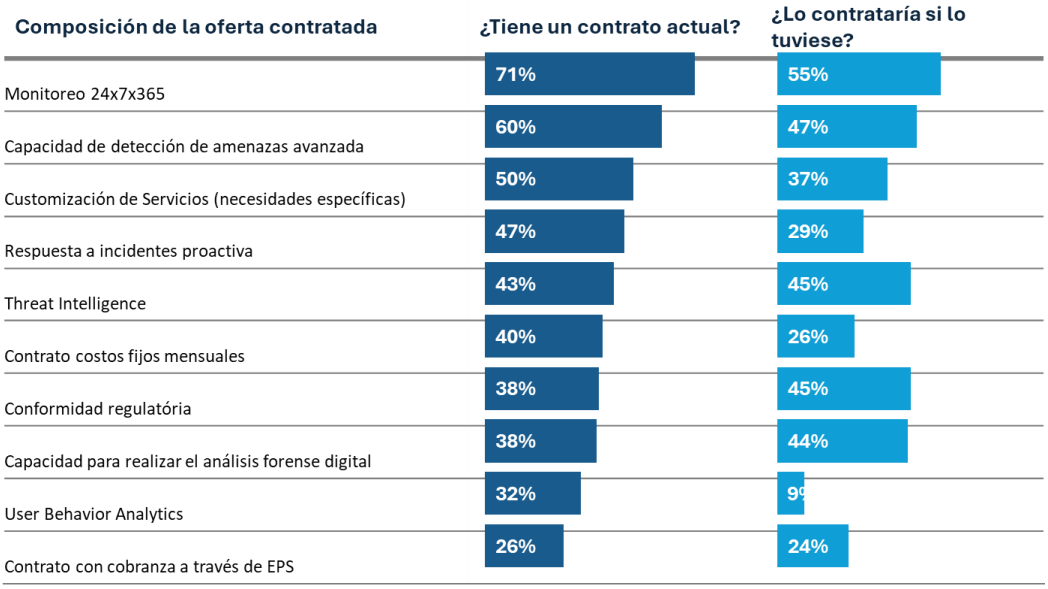
Aunque existen diferencias sutiles, las tres primeras razones indicadas en la Figura 5 se consideran prioritarias, ya que la diferencia de puntuación es mínima (2,53, 2,51 y 2,50 en una escala que llega a 3). Estos factores pusieron en evidencia las preocupaciones de un mercado que se está moviendo rápidamente hacia una mayor madurez en Seguridad.

Un dato interesante es que, en la búsqueda del expertise, las estructuras SOC geográficamente cercanas y los equipos que hablan el mismo idioma tienen poco peso a la hora de decidir por la contratación de proveedores de servicios gestionados de seguridad.

Es importante mencionar que 48% de las empresas consultadas señalaron que sus contratos incluyen servicios relacionados con SOC[5]. También es interesante mencionar que hay interés y demanda de diversos ítems complementarios a los servicios usualmente ofertados en los contratos estándar de SOC. La Figura 6 muestra que el segundo ítem más contratado (que también es el segundo elemento que las empresas no contratistas contratarían más si esto fuera posible con su proveedor actual) es la capacidad de detectar amenazas avanzadas. Del 40% de las empresas que no tienen este ítem en su contrato, poco menos de la mitad, 47%, indicó que sí lo contratarían si el proveedor actual les ofreciera esta posibilidad.

[5] *Security Operations Center- o centro de operaciones de seguridad es un equipo interno o externo de profesionales de seguridad informática que supervisan toda la infraestructura tecnológica de una organización las 24 horas del día.*

FIGURA 6: **Ítems complementarios a los servicios que se suelen ofrecer en los contratos estándar de SOC**



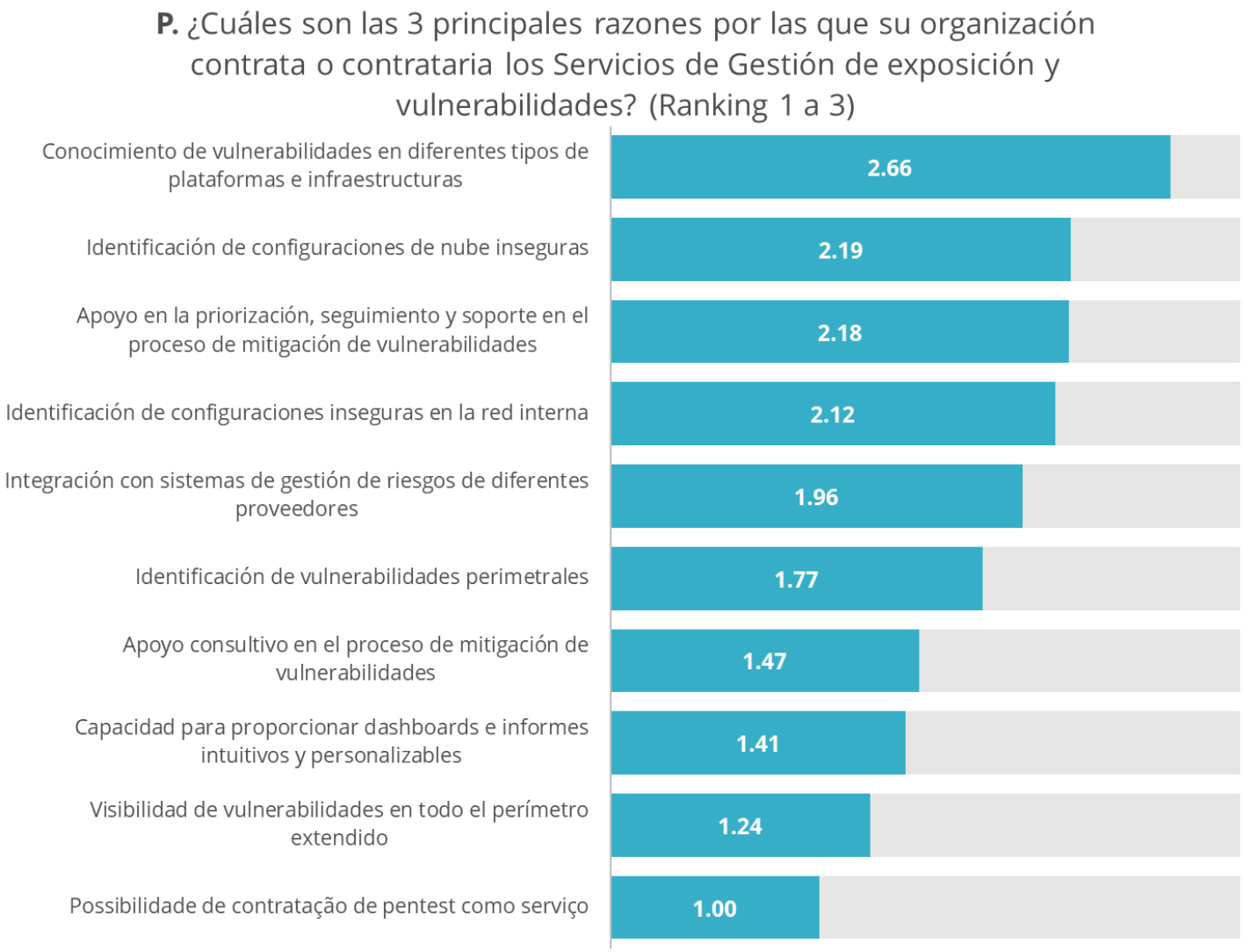
Fuente: IDC Brasil, Adoção de Serviços Gerenciados de Segurança, 2023.

Threat Intelligence,[6] el cumplimiento normativo y la capacidad de realizar Análisis Forense Digital son elementos que generan interés y estarían bajo el mismo contrato, si fuera posible con el proveedor actual. Sin duda, para aprovechar las tecnologías, el conocimiento regulatorio y el análisis profundo, las organizaciones deben confiar en un proveedor de servicios gestionados y un consultor en su viaje hacia una estrategia de seguridad más integral.

En cuanto a las principales razones (Figura 7) para contratar servicios de gestión y exposición de vulnerabilidades, las organizaciones buscan principalmente el conocimiento y la capacidad para soportar y monitorear vulnerabilidades en diversas plataformas e infraestructuras. Además, el proveedor de servicios gestionados de seguridad debe ser capaz de identificar configuraciones que puedan resultar riesgosas en entornos de nube y apoyar al cliente en los procesos de identificación y mitigación de posibles vulnerabilidades.

[6] *Threat Intelligence*- ou inteligência de ameaças cibernéticas é a análise de um conjunto de dados para identificar riscos cibernéticos em potencial e definir as melhores ações de segurança para uma empresa.

FIGURA 7: **Razones para adquirir los servicios de gestión y exposición de vulnerabilidades**



Fuente: IDC Brasil, Adoção de Serviços Gerenciados de Segurança, 2023.

IV. Consideraciones sobre MDR

Managed Detection and Response (MDR) es un modelo de servicio de seguridad con un enfoque más avanzado para detectar y responder a las amenazas a través de tecnologías como el *Machine Learning* y la Inteligencia Artificial para identificar actividades sospechosas y poder responder a estas amenazas en tiempo real, minimizando el impacto del ataque.

Según el estudio, para poco más de una cuarta parte de las organizaciones (26%), los servicios MDR son vistos como una evolución de los servicios de seguridad gestionados tradicionales. Según 22% de las organizaciones, los servicios MDR son

mejores para detectar y responder a amenazas avanzadas a un ritmo automatizado y más rápido en comparación con los servicios de seguridad gestionados tradicionales. Sin embargo, estos puntos de vista muestran cierta limitación en el conocimiento de lo que el MDR es capaz de ofrecer. Las organizaciones deben considerar las ventajas de MDR, particularmente en la capacidad y efectividad en la detección avanzada de amenazas, el monitoreo continuo de la tasa de detección y la precisión para identificar las amenazas, la inteligencia de amenazas y la capacidad de reducir el tiempo promedio hasta la detección y respuesta a los incidentes (MTTD - Mean Time to Detection / MTTR - Mean Time to Respond).

Otro estudio de IDC, realizado en septiembre de 2023 con 110 tomadores de decisiones, *IDC Latin America: Managed Detection and Response (MDR) Survey,* muestra que los tres ítems principales considerados al elegir un proveedor de servicios MDR son: capacidades adyacentes, superioridad funcional y reconocimiento de marca. . El factor costos quedó en cuarto lugar. Otro punto importante que muestra cómo los servicios MDR son un beneficio con un futuro prometedor es que 70% de las organizaciones están de acuerdo en que su proveedor de MDR ofrece una cartera completa, que puede combinarse con servicios de seguridad adyacentes.

En entornos digitales, los principios de confianza mínima y otras características vinculadas a la gestión de identidades y accesos deben ser comprendidos por los gestores de Seguridad, especialmente cuando el 65% de las organizaciones no han implementado una estrategia Zero Trust[7], dejando la oportunidad de beneficiarse de numerosas ventajas, tales como una mejor gestión de vulnerabilidades y pruebas en general (simulación de ataques de intrusión y penetración), mayor seguridad y gobernanza de datos, protección de vulnerabilidades internas (detrás del firewall) y limitación de la propagación de cualquier ataque exitoso.

V. Conclusiones

Los servicios y soluciones enfocados en la seguridad de la información no son una opción. Se trata de iniciativas necesarias para las organizaciones, independientemente de su tamaño, vertical o ubicación geográfica. Aunque el estudio que sirvió de base para este documento (IDC Brasil, Adoção de Serviços Gerenciados de Segurança, 20233) muestra un grado satisfactorio en el entendimiento del rol de la seguridad en las empresas consultadas, hay oportunidad para evolucionar en todas las geografías incluidas en la encuesta en LATAM.

IDC considera que, para alcanzar una mayor madurez, aumentar las capacidades de defensa y alcanzar un buen nivel de resiliencia cibernética, uno de los caminos que se pueden seguir con mayor asertividad es establecer alianzas con proveedores de Servicios Gestionados. Se debe tener capacidad para evaluar e implementar, junto con los equipos propios de las organizaciones, las medidas y soluciones necesarias para

La investigación mostró que, incluso frente a numerosos desafíos, el camino hacia la madurez y la resiliencia cibernéticas se basa en la alianza, el apoyo y el *know-how* de los proveedores de servicios de seguridad gestionados.

Luiz Monteiro, IDC Brasil

[7] Zero Trust- es un acercamiento arquitectónico y una meta para la seguridad que supone que cada transacción, entidad e identidad no es confiable hasta se establece y se mantiene a lo largo del tempo.

aumentar las barreras de entrada ante las ciberamenazas y violaciones cibernéticas.

El uso de proveedores de seguridad gestionados con una amplia cartera de servicios y herramientas puede fortalecer la inteligencia contra posibles ataques y mejorar el monitoreo, el análisis y la respuesta a incidentes de seguridad. Por lo tanto, contar con un socio con las credenciales adecuadas puede facilitar y minimizar, enormemente, los esfuerzos necesarios para mantener las estructuras corporativas alejadas de los múltiples inconvenientes que pueden ocurrir debido a invasiones con objetivos maliciosos y criminales.

Acerca del Analista

Luiz Monteiro, Analista Sénior del Mercado de Servicios, IDC Brasil

Luiz Monteiro es Analista de Investigación y Consultoría en IDC, cubriendo el mercado brasileño, sus organizaciones y proveedores. Los estudios realizados por el equipo de servicios de TI brindan a los clientes de IDC una visión detallada sobre el tamaño del mercado, el análisis de competidores y los pronósticos en el mercado de servicios de TI en el país.

MENSAJE DEL PATROCINADOR

Los servicios gestionados de seguridad han sufrido un cambio vertiginoso en los últimos años. La incorporación de variados tipos de tecnologías, prácticas y know-how han sido uno de los factores de dinamismo para la industria que han generado una brecha entre los actuales servicios de Detección y Respuesta a los tradicionales servicios gestionados de monitoreo de seguridad. SEK ha querido contribuir al mercado latinoamericano al patrocinar este estudio con el objetivo de facilitar la toma de decisiones y la comprensión de nuestra propia madurez en este relevante ámbito.

IDC Brasil
Av. Eng. Luís Carlos Berrini 1645,
São Paulo, SP, 04571-011
+55 11 5508-3400
Twitter: @IDCLatin
www.idclatin.com
www.idc.com

IDC Custom Solutions

International Data Corporation (IDC) es la principal firma mundial de inteligencia de mercado, servicios de consultoría, y eventos para los mercados de Tecnologías de la Información, Telecomunicaciones y Tecnología de Consumo.

Con más de 1,100 analistas alrededor del mundo, IDC provee experiencia mundial, regional y local sobre las tendencias y oportunidades en tecnología e industria en 110 países.

El análisis y conocimiento de IDC ayuda a los profesionales de TI, ejecutivos de negocios y la comunidad de inversión, a tomar decisiones fundamentadas sobre tecnología y a alcanzar los objetivos clave de negocio.

Fundada en 1964, IDC es una subsidiaria de IDG, la empresa líder en medios de tecnología, investigación y eventos.

Para conocer más acerca de IDC, por favor visita www.idc.com y www.idclatin.com

Síguenos en Twitter como @IDCLatin / @IDC