IDC SPOTLIGHT
*Patrocinado por: Sophos*

**El objetivo de cualquier servicio de ciberseguridad incluyendo los MDR, es reducir la carga de trabajo de los equipos de seguridad, dar escalabilidad y eficiencia de costos.**

# MDR, la propuesta a la necesidad de mejores habilidades de detección y respuesta

*Marzo, 2023.*

**Escrito por:** Emanuel Figueroa, Analista Senior de Inteligencia de Mercado de Seguridad, Enterprise, IDC América Latina.

## *I. Cambios en las iniciativas enfocadas a la entrega de servicios digitales*

Con la comprensión de las organizaciones de incorporar competencias a sus modelos de negocio, después de las más recientes crisis, el giro en las prioridades de los líderes del negocio continúa siendo impulsada por la tecnología.

En el caso de América Latina, el 44%[1] de las organizaciones considera aumentar la productividad; 34% enfocará sus esfuerzos en mejorar la retención y adquisición de clientes y, en su esfuerzo por lograrlo, 33% centrará sus esfuerzos en combinar experiencias de usuario físico-digitales y ubicar al cliente en el centro de sus productos y servicios.

Debido a la agilidad y nuevas dinámicas con las que el mercado demanda productos y servicios, se han multiplicado los proyectos que incorporan tecnología para soportar estos objetivos y mejorar la calidad de sus decisiones, a la vez que soportan el proceso de digitalización de las compañías. De acuerdo con un estudio elaborado por IDC, según la importancia estratégica en las iniciativas de TI de 424 organizaciones, el 45% de las organizaciones considera la Ciberseguridad como el atributo más importante, seguido de la gestión de nube y TI hibrida (31%), y movilidad (26%, incluyendo gestión de dispositivos, aplicaciones y desarrollo móvil).

Otro elemento que induce a un cambio en el comportamiento del mercado, en relación con la entrega de los servicios digitales, es el interés por consumir de entidades que satisfagan nuevos criterios de compra como la responsabilidad social y la confianza digital.

*[1] Fuente: IDC Latin America Investment Trends – CIO Agenda and Budget, n=424.*
*[2] Fuente: IDC Latin America Cyber Security Report 2022, n=653.*

## EN UNA MIRADA

### DATOS ESTADÍSTICOS

- Cambios en la estrategia de negocios que impulsan la adopción en la iniciativa de Ciberseguridad: 48.4%[2] se enfocan en mejorar la experiencia de sus clientes; 48.2%, en fortalecer sus canales digitales debido al impacto en la retención de clientes; 43% en habilitar sus competencias de trabajo remoto/trabajo desde casa.
- El principal cambio en la dinámica de trabajo a distancia impulsó a 58.8% de las organizaciones a agregar a sus operaciones de TI, monitoreo, alertamiento y gestión remota. 57.6% incorporaron entrenamiento para generar conciencia de Ciberseguridad para empleados no técnicos.
- Siete de cada diez organizaciones cuentan con hasta dos colaboradores para atender las necesidades de ciberseguridad de sus negocios, haciendo que 55% de las empresas adquieran algún tipo de contrato para extender sus equipos operativos y repartir la carga con un tercero.
- Después de los requerimientos de cumplimiento y el soporte 24x7, la razón más importante para contratar servicios gestionados de Ciberseguridad son las capacidades de detección y respuesta.

## *El impacto en la inversión en la infraestructura que soporta la digitalización*

Los procesos de digitalización de servicios y experiencias están impactando en la asignación de presupuesto de TI donde, hacia fines del 2022, 61% de la inversión (Figura 1) estará destinándose a ambientes en el sitio de un proveedor de servicios de TI, y se prevé que el consumo de servicios de nube pública siga acelerándose hasta alcanzar un crecimiento de 43%[3] con respecto al año anterior.

FIGURA 1: ***Asignación de presupuestos de TI***

*América Latina, 2019 y 2022*


*Fuente: IDC Latin America Investment Trends Survey Diciembre 2019 – Enero 2022.*

Esto significa que gran parte de la digitalización se sustenta en la aceleración en el consumo como servicio, dentro del que podemos citar el consumo de nube pública e iniciativas de nube privada, tanto en ambientes *on-premise* como los ofrecidos por terceros en sus centros de datos locales, y el consumo de los diversos modelos de servicio IaaS, PaaS y SaaS con más de un proveedor, definiendo así además una tendencia de inversión hacia el no tan nuevo pero popular perfil *multicloud*.

Este panorama nos indica que los activos están cada vez más dispersos, conectados por aplicaciones y plataformas de colaboración, en ambientes híbridos y se debe tener consciencia de los nuevos modelos de Ciberseguridad que las organizaciones deberán implementar como parte de la responsabilidad que comparten junto a los proveedores de servicios de nube.

Es clave el entendimiento del alcance de la Ciberseguridad más allá de las estrategias de modernización en la nube; es decir entender que las nuevas plataformas agregadas como parte de la modernización de los negocios requerirán de asegurar los nuevos activos, flujos de comunicación y el nuevo volumen de datos requeridos para tomar decisiones, reducir riesgos y cumplir con objetivos de responsabilidad digital con la nueva generación de consumidores, que es cada vez más consciente del valor de sus datos personales.

[3] *Fuente: IDC Semianual Public Cloud Services Tracker 2022H1.*

### *La Confianza Digital como valor diferenciador de la organización*

Para IDC, la Confianza Digital es la condición para la toma de decisiones entre dos o más partes, que refleja el nivel de confianza (riesgo y reputación) entre ellas, minimizando los riesgos, implementando estrategias de Ciberseguridad y cumplimiento, al mismo tiempo que se protege la privacidad de empresa, empleados, proveedores, socios de negocio y clientes, conduciéndose hacia la ética y la responsabilidad social, de ahí que la confianza digital se vuelve un valor diferenciador de la organización.

Para poder desarrollarla, las organizaciones deben analizar el foco de su negocio y evaluar soluciones y servicios orientados a una correcta gestión de riesgos transversal a la organización y a la optimización de las capacidades de Ciberseguridad, además a la creación de una infraestructura que garantice su ciber-resiliencia y mejora continua.

FIGURA 2: ***Confianza Digital***


*Fuente: IDC.*

Como se había mencionado antes, las organizaciones de América Latina han mostrado ya un creciente interés en los programas de Confianza Digital dentro de sus principales iniciativas de negocio. De acuerdo con el estudio IDC Latin America Investment Trends de 2022, 16.2% de las empresas impulsarán la iniciativa de enfocarse en la protección de los derechos de privacidad, especialmente cuando nuevas regulaciones y requerimientos influyen en las prácticas de gobierno de datos. Tal es el caso de las leyes de protección de datos en América Latina y los diferentes enfoques que se han adoptado en la región. En ese sentido, es posible citar algunos ejemplos: en Brasil con una adecuación de su Ley General de Protección de Datos Personales (LGPD) al modelo europeo de GDPR, que ya se encuentra vigente y con sanciones punitivas de hasta el 2% de sus ingresos desde agosto del 2021. En esa misma línea se encuentra Ecuador quien, a partir de mayo de 2023, podrá multar con hasta el 1% de su facturación a las entidades públicas o privadas por mal manejo de los datos personales.

En México, con su LFPDPPP[4], multó entre 2021 y 2022 el equivalente aproximado de 7.5 millones de dólares. Esta dinámica muestra el avance de algunos países de la región de articular la confianza en el tratamiento de los datos como un derecho de todos los ciudadanos.

La realidad es que, aunque muchas de las empresas aún no han logrado avances en la implementación de sus programas de privacidad, el daño reputacional es la primera preocupación para una de cada cuatro empresas en América Latina, sin embargo, la tendencia global para los siguientes años será el de mantener un uso responsable de los datos. No obstante, esta situación generará una oportunidad para las empresas que puedan articular esta práctica como medida de retención de clientes.

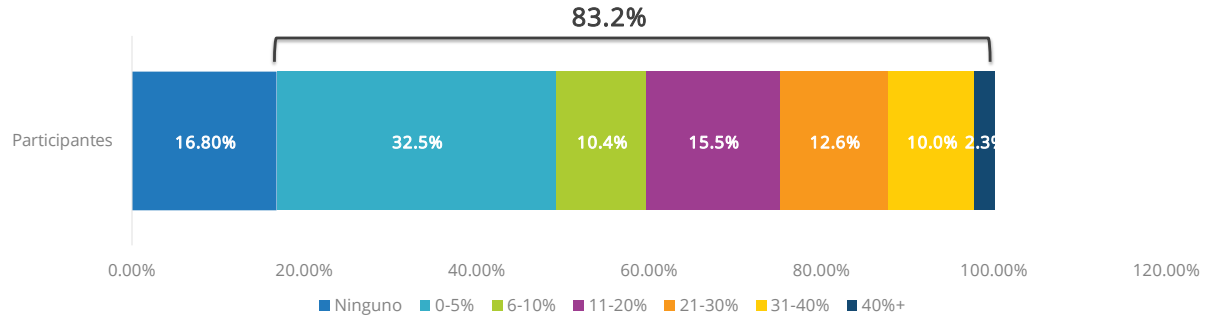
Otro aspecto relevante, relacionado a los retos que los CIO y directores de TI están enfrentando y que pueden complicar las iniciativas de programas de Confianza Digital, es la necesidad de atender la deuda tecnológica acumulada desde el inicio de la crisis sanitaria y que en muchos casos se ha visto extendida por el consumo de servicios de nube sin haber resuelto completamente las brechas generadas a inicios del 2020. Desde el pilar de Ciberseguridad, dentro de la pirámide de la Confianza Digital, observamos que las organizaciones empiezan a considerar soluciones y servicios gestionados que les brinden visibilidad, atiendan necesidades de orquestación de infraestructura y les ofrezcan niveles de automatización que permitan reducir el estrés de los equipos especializados de Ciberseguridad.

La confianza digital es clave en el éxito de las organizaciones y un atributo relevante para sus clientes y socios de negocio, no solo relacionado con la reputación de la compañía, sino también con factores como la transparencia, fiabilidad y privacidad en el tratamiento de los datos, permitiendo diferenciar a las organizaciones que adopten estos elementos y engendrando un nuevo criterio de elección al comprar o establecer una relación de negocio.

## *II. El modelo extendido de operación reta los modelos tradicionales de Ciberseguridad.*

Al 2024, se espera que el 83.2%[5] de organizaciones tenga parte de su fuerza de trabajo de forma remota para reducir costos relacionados con el uso de oficinas, dotar de movilidad a sus equipos, además de servir como incentivo de un mejor balance vida-trabajo para sus colaboradores.

FIGURA 3: ***Porcentaje de colaboradores trabajando de forma remota/trabajo desde casa en los siguientes 3 años.*** *América Latina, 2022-2024.*




*Fuente: IDC Latin America Cyber Security Report 2022, n=653*

[4] *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.*

[5] *Fuente: IDC Latin America Cyber Security Report 2022, n=653.*

Esta dinámica de trabajo ha impulsado a las organizaciones a evaluar sus arquitecturas de Ciberseguridad y así extender sus capacidades más allá de sus centros de datos, a pesar de ello, a medida que las herramientas de Ciberseguridad cubren nuevas áreas para soportar la operación, la asimetría entre las alertas generadas por cada solución y el aumento en sus cargas de trabajo ponen a prueba la habilidad de los analistas de Ciberseguridad para detectar y contener incidentes. Siete de cada diez[6] organizaciones cuenta con hasta dos colaboradores para atender las necesidades de Ciberseguridad de sus negocios, haciendo que 55% de las empresas adquieran algún tipo de contrato para extender sus equipos operativos y repartir la carga con un tercero.

De acuerdo con el más reciente estudio de (ISC)2 respecto a la fuerza de trabajo, se estima que en el mundo existe una brecha de profesionales de ciberseguridad de 3.4[7] millones de trabajos, en América Latina se estiman 515,879, lo que representa el 15% de la proyección global en áreas como evaluación de riesgos, vigilancia y gestión de parches de sistemas críticos. Donde la mitad de los colaboradores encuestados consideran que el déficit de recursos pone a la empresa en un riesgo moderado a extremo de ciberataques.

En términos de competencias, la generación de nuevos canales ha mejorado las posibilidades de ingreso de las compañías, al tiempo que demanda nuevas plataformas tecnológicas que soporten estas iniciativas, y genera importantes volúmenes de datos con gran valor para la toma de decisiones, cambiando su residencia, brinda continuidad operativa y amplía el reto de las áreas responsables de Ciberseguridad de asegurar y proporcionar correcto tratamiento a la información en uso, tránsito y reposo, considerando la velocidad a la que se replican y almacenan los datos.

Con la creación de nuevos flujos de ingresos por servicios digitales y la distribución de sus entornos, la privacidad toma un papel importante para los consumidores, quienes más conscientes del valor de sus datos buscan exponerse al menor riesgo al consumir bienes y servicios de empresas que garanticen ese derecho. Al consultar a más de 650 organizaciones de América Latina por la residencia de sus datos críticos, 34%[8] hospeda la mayoría de sus datos críticos en ambientes de Big Data, el 33% en herramientas de colaboración y 30% en aplicaciones SaaS por citar algunos ejemplos.

Para abordar estas preocupaciones, el 45.8%[9] de las organizaciones encuestadas comparte que gastó hasta el 25% de su presupuesto de Ciberseguridad de red en soluciones Secure Defined Secure Access (SDSA), como parte de sus iniciativas de asegurar los accesos de sus recursos a distancia. Otras organizaciones han adoptado nuevas prácticas como la Ciberseguridad en el desarrollo de software (DevSecOps) donde 57.4% de los consultados la identifica como la principal razón de reducción del riesgo al usar plataformas de nube, y 55.6% incorporó una estrategia de confianza cero (Zero Trust) para proteger su red interna contra vulnerabilidades de su red extendida.

Bajo este contexto las organizaciones deben considerar que tal distribución aumenta la carga de trabajo de toda la empresa, aunque para soportar la continuidad y experiencia de uso, la oficina de Ciberseguridad juega un papel importante, por ejemplo los arquitectos de Ciberseguridad deberán asignar tiempo a la implementación de nuevas soluciones y casos de uso, a nivel de operaciones de Ciberseguridad aumenta la cantidad de tiempo invertido en actividades como monitoreo de alertas, *triage* y asignación de casos de investigación con cada herramienta de Ciberseguridad añadida, a la vez que reta las competencias existentes para adoptar nuevos *frameworks* como el modelado de amenazas de STRIDE[10] o MITRE[11], y en la mayoría de los

*[6] Fuente: IDC Latin America Cyber Security Report 2022, n=653.*
*[7] Fuente: International Information System Security Certification Consortium (ISC)[2] Cybersecurity workforce study 2022.*
*[8] Ibid [6]*
*[9] Ibid [6]*
*[10] MITRE ATTA&CK refiere a MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT & CK), el cual es la base de conocimiento y modelo sobre el comportamiento del adversario cibernético, desde el ciclo de vida del ataque y las plataformas a las que se dirige.*
*[11] STRIDE refiere a un modelo de amenazas para ayudar a razonar y encontrar amenazas a un sistema.*

casos, para los responsables de ciberseguridad, incrementa la consideración por extender sus contratos de servicios gestionados para hacerle frente a estas nuevas tareas y competencias requeridas.

Los servicios gestionados, por otra parte, contribuyen a resolver retos como: la rotación de colaboradores, la velocidad y capacidades para gestionar los cambios, la interpretación de indicadores de compromiso (IOC's) y reducir los tiempos de detección de amenazas con mayor impacto para el negocio. El 37.7%[12] de las empresas considera que la detección y respuesta es la razón que habilita la contratación servicios gestionados de Ciberseguridad, 31.5% considera además la falta de experiencia en los recursos internos y 28.8% la experiencia en cacería de amenazas o *Threat hunting.*

Otro aspecto que reta a los modelos de Ciberseguridad existentes es que con cada proyecto se reduce el ancho de banda de los equipos de Ciberseguridad, quienes pasan la mayor parte de su tiempo cubriendo requerimientos de cumplimiento. El 39%[13] de las compañías que contrataron servicios de consultoría de ciberseguridad invirtieron en el desarrollo de *playbooks* de respuesta a incidentes para soportar sus planes de preparación contra brechas; 51% de los servicios de implementación fueron contratados para ayudar en el diseño de la arquitectura de Ciberseguridad, dando paso a una nueva generación de servicios gestionados.

### *La necesidad de automatizar procesos de Ciberseguridad*

De acuerdo con el estudio IDC Latin America Cyber Security Report 2022, la automatización de la Ciberseguridad está dentro de las primeras dos prioridades para 52% de las organizaciones en América Latina, en que se incluye la automatización de analítica de Ciberseguridad, del control de accesos, de la detección de intrusión y de herramientas para cumplimiento, auditoría y SIEM (*Security Information and Event Management*, gestión de eventos de seguridad de la información).

Para alcanzar los niveles de automatización de Ciberseguridad necesarios, se debe hacer un uso efectivo de presupuestos, considerando priorizar la contratación de servicios. Actualmente, el 83%[14] de las empresas siguen enfrentando retos de contratación de profesionales de Ciberseguridad, razón por la que el 55% de las organizaciones tienen contratos de servicios y continuarán creciendo. En esta situación, las empresas deben aprovechar la automatización en los servicios de Ciberseguridad para el monitoreo, recolección, correlación, análisis, detección, reporte y respuesta a incidentes y amenazas avanzadas.

## *III. La evolución de los servicios gestionados y su enfoque en resultados.*

Hoy en día las compañías entienden que gestionar las configuraciones de sus herramientas son solo el primer nivel en el proceso de operaciones de seguridad (SOC). A medida que las amenazas se han sofisticado, la necesidad de contar con más habilidades para contener los potenciales incidentes ha impulsado cambios en la industria, los Managed Security Service Provider (MSSP) incorporaron competencias de detección, acuñando el término de *Managed Detection and Response (MDR),* por la integración plataformas de inteligencia de amenazas, análisis de comportamiento de usuario y capacidad de cacería de amenazas, análisis predictivo y respuesta automatizada, entre otros.

Y es que las organizaciones han comprendido que el objetivo de cualquier servicio de Ciberseguridad, incluyendo los MDR, es resolver sus necesidades particulares como reducir la carga de trabajo de los equipos de ciberseguridad, dar escalabilidad y eficiencia de costos, más allá de solo concentrarse en los atributos que ofrece uno u otro.

*[12] Fuente: IDC Latin America Cyber Security Report 2022, n=653.*
*[13] Ibid*
*[14] Ibid*

Algunos KPIs como el tiempo promedio de detección (MTTD) o tiempo promedio de reparación (MTTR) impulsados por la industria de correlación de eventos han generado conciencia en las empresas que ahora construyen sus programas de Ciberseguridad alrededor de estos indicadores. Una de cada cuatro[15] compañías de manufactura resalta la importancia de mejorar estos valores en su decisión por adquirir servicios gestionados, agregando a su lista de criterios la comparación entre tiempos de respuesta ante incidentes, el aumento en la visibilidad y entendimiento del ecosistema de la organización, así como también *expertise* y competencias específicas en los equipos de Ciberseguridad, desde un nivel de evolución Tier 1[16], hasta el nivel Tier 3 en la evolución de los servicios de Ciberseguridad:

- Tier 1: esta generación de servicios busca gestionar la configuración del set de herramientas primordial como el antivirus, firewall, IDS, seguridad en email, monitoreo de salud de los equipos y escaneo de vulnerabilidades.
- Tier 2: incorpora la detección, monitoreo y alertas continuas en una base de 24 x 7; la Tercerización y/o administración compartida de SIEM, NGFW/UTM, EDR, TISS, analítica y detección avanzada, tickets de TI con Machine Learning/Inteligencia Artificial y servicios complementarios.
- Tier 3: la necesidad de generar eficiencias en los controles de Ciberseguridad da paso a un enfoque con conocimiento contextual, UEBA avanzado, respuesta automatizada, enfoque predictivo, forense, respuesta a incidentes, caza de amenazas, riesgo asociado a terceros, *zero trust* e integración de plataformas.

### *Managed Detection & Response*

Para IDC, MDR es componente de *Managed Security Services* (servicios gestionados de seguridad) que combina herramientas, tecnologías, procedimientos y metodologías para brindar capacidades integrales de detección y respuesta de Ciberseguridad. Los proveedores de servicios pueden ofrecer MDR combinando las capacidades existentes de la empresa con herramientas y servicios de sus socios tecnológicos y su propiedad intelectual. Típicamente, los servicios de MDR son proporcionados por personal calificado en Ciberseguridad que trabaja en un centro de operaciones de seguridad (SOC, *security operations center*) con disponibilidad de 24x7x365. La Figura 4 muestra los elementos de MDR para la entrega de valor, impacto y los resultados esperados en Ciberseguridad, con base en las siguientes capacidades:

- Uso de las capacidades de protección de *endpoints* como parte de un sistema EDR. XDR, con acceso a los datos como la telemetría de red, nube o los sistemas de mensajería, en lugar de un sistema EDR.
- Integración de múltiples fuentes de inteligencia de amenazas para proporcionar información oportuna en el servicio MDR. El objetivo es permitir a las organizaciones comprender qué sistemas son los objetivos, quién está apuntando al objetivo y las tácticas, técnicas y procedimientos que son vitales en el cambio de la ciberseguridad de una postura reactiva a una postura proactiva.
- Uso regular de la caza de amenazas (*threat hunting*) manejada por humanos para complementar las amenazas descubiertas por los IoC (*Indicators of Compromise*), con base en el análisis de riesgos y/o inteligencia de amenazas.
- Servicios de respuesta remota a incidentes, incluyendo la contención y eliminación de adversarios, incidentes o intrusiones en los que se sospecha o se sabe que los datos han sido filtrados, destruidos o manipulados. IDC considera que una parte central del servicio MDR debe ir más allá de ofrecer orientación y recomendaciones y

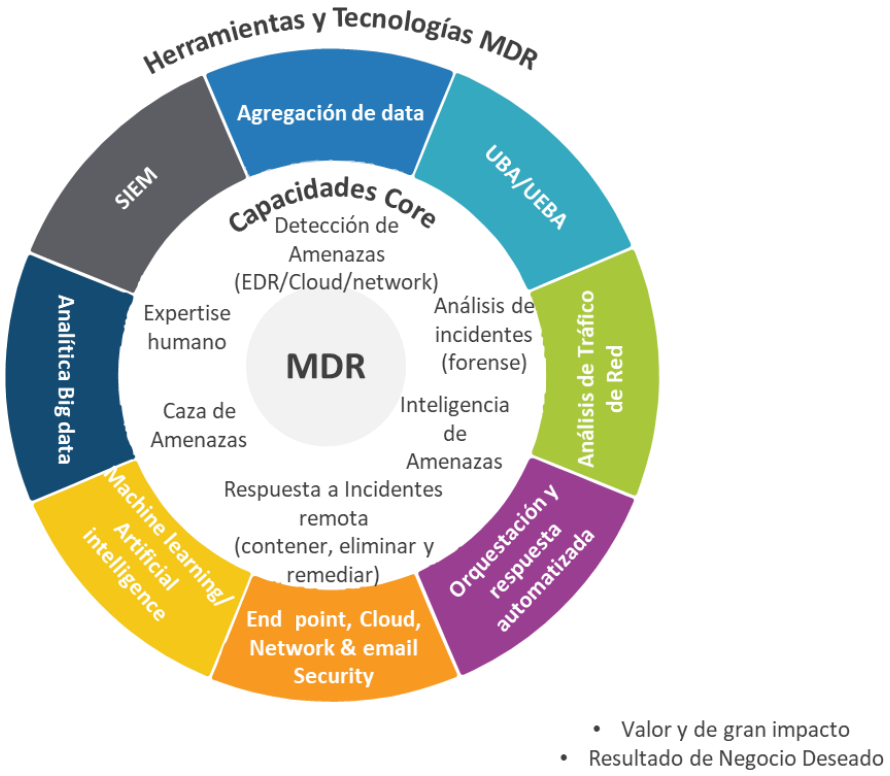
[15] *Fuente: IDC Latin America Cyber Security Report 2022, n=653.*

[16] *Fuente: IDC MDR: The next Generation of Managed Sercurity Services – June 2020.*

debe incluir un componente que pueda automatizar una respuesta para el cliente cuando se descarga *malware* sin que haya otro daño colateral.

- Servicios integrales de respuesta remota a incidentes (con cargo adicional) para violaciones graves que requieren una respuesta coordinada, remediación y capacidad forense.
- Tableros basados en web que permiten el monitoreo, la actualización y la generación de informes de todos los IoC que se crean desde el servicio.

FIGURA 4: ***Estructura de una Solución de MDR***




*Fuente: IDC.*

## *III. Beneficios de MDR*

Los servicios MDR permiten a las organizaciones mantener un nivel constante de conciencia y protección, junto con la flexibilidad para volver a priorizar, reevaluar y reconfigurar los riesgos, así como las tolerancias y actividades de detección y respuesta. Cada vez más, los estrategas de seguridad ven a MDR como una necesidad para ayudarles a madurar sus programas de ciberseguridad. Los beneficios de MDR se reflejan en:

- Procesos de automatización y flujos de trabajo que agilizan la detección, especialmente con la capacidad del proveedor de normalizar, enriquecer y analizar los datos de diversas fuentes.
- Traslada competencias sofisticadas de identificación, detección y contención de amenazas sin comprometer la precisión de las operaciones, creando un balance entre: la calificación del personal y la eficiencia en costos.

- Aprovechamiento de los recursos existentes, de manera que las organizaciones no requieren reemplazar tecnologías para eliminar los puntos ciegos para fortalecer sus defensas.
- Repuesta gestionada, con guía de remediación para que las organizaciones puedan emprender acciones oportunas. Los equipos de Ciberseguridad pueden prepararse para anticiparse y atender algún incidente en forma inmediata.
- Soporte en incidentes, que permite transferir la respuesta a incidentes al proveedor de servicio de Ciberseguridad.
- Capacidad de respuesta en ambientes de nube, con análisis forense, causa raíz y correlación de eventos.
- Inteligencia de amenazas para hallar en forma más inmediata las amenazas en el ambiente de la empresa.
- Base de conocimiento de acciones y campañas de los atacantes.
- Apoyo en la definición y ejecución de un mapa de ruta de Ciberseguridad integral.

IDC recomienda a las organizaciones evaluar los proveedores de MDR con base en los resultados esperados en la detección y respuesta cotidiana y el estado del arte de la empresa; sobre todo porque estamos siendo testigos de un incremento, no sólo del número de ataques, sino en la complejidad de éstos que impactan a las organizaciones de América Latina.

En el último reporte de Ciberseguridad para América Latina de IDC del 2022, se encontró que las organizaciones seguían identificando los orígenes de un evento de ciberseguridad en actividades relacionadas a errores de configuración de servicios de nube, phishing y vulnerabilidades que no habían sido parchadas y que permitieron el ingreso de *malware* a los ecosistemas de la organización. En el mismo reporte, IDC encontró que 26.4% de las organizaciones de la región identificaban los altos costos de contratación de personal calificado y la falta de conocimiento especializado, como las principales dificultades al momento de buscar contratar profesionales de ciberseguridad. Sin duda esto tiene un impacto muy alto en lo referente a la capacidad de una organización para responder ante las amenazas de forma efectiva, los servicios de MDR se configuran como una alternativa que puede ayudar a la oficina del CISO y a su equipo a estar mejor preparados.

## *V. Sophos y su propuesta de MDR*

Sophos es una empresa global de software y hardware de Ciberseguridad, que actualmente protege más de 400 000 organizaciones de todos los tamaños en más de 150 países. Con la tecnología de SophosLabs, sus soluciones nativas de la nube y mejoradas con IA pueden adaptarse y evolucionar para proteger los puntos finales y las redes contra tácticas y técnicas cibercriminales. Administrados a través de su plataforma basada en la nube, Sophos Central, sus productos trabajan juntos a través de su sistema de seguridad sincronizada para compartir inteligencia sobre amenazas y responder a las amenazas en evolución. El conjunto de productos de Sophos está diseñado para proteger las redes y los puntos finales contra infracciones automáticas y de adversarios activos, ransomware, malware, exploits, exfiltración de datos, phishing y más.

La solución MDR de Sophos parte de la idea de que *Endpoint Detection and Response* (EDR) es una tecnología que monitorea y responde continuamente para mitigar las amenazas cibernéticas, pero que requiere de personal experto para su mayor aprovechamiento a través de los servicios de Ciberseguridad gestionados, específicamente los servicios de detección y respuesta gestionadas (Managed Detection and Response, MDR). Estos servicios actúan como una extensión

del equipo de Ciberseguridad de la organización que combina el conocimiento de investigaciones realizadas por seres humanos, la búsqueda de amenazas, la supervisión en tiempo real y la respuesta a incidentes con el apoyo de tecnologías avanzadas en host y redes para recopilar y analizar información. Esto cobra relevancia si consideramos que los controles preventivos (antivirus, *firewalls*, filtrado de contenido) normalmente pueden ser eficaces para detener amenazas conocidas, pero no contra los ciberataques nuevos y sofisticados. De ahí que en la propuesta de Sophos se destacan:

- Servicio Sophos Managed Detection and Response (MDR)— servicio totalmente administrado por un equipo de 500 expertos en seis centros globales de operación que ofrece funciones de búsqueda, detección y respuesta a amenazas las 24 horas. Más allá de la notificación de ataques o comportamientos sospechosos, el equipo de Sophos MDR adopta medidas específicas para neutralizar incluso las amenazas más sofisticadas y complejas, con analistas enfocados en descubrir indicadores de compromiso, producir inteligencia basada en ciencia de datos y revelar el mapa de ruta de los ataques. La opción MDR avanzada comprende búsqueda de amenazas sin pistas las 24 horas, investigaciones de amenazas con apoyo de telemetría, un responsable de respuesta ante amenazas dedicado que colabora con los recursos locales de la organización. La modalidad de Sophos Rapid Response— es el servicio de un equipo de expertos en respuesta a incidentes, con asistencia rápida para identificar y neutralizar amenazas activas contra la empresa. El servicio Rapid Response se ofrece a las empresas que están siendo atacadas para clasificar, contener y neutralizar amenazas activas, expulsión de adversarios, supervisión y respuesta 24/7 y acciones preventivas en tiempo real.

- Sophos MDR, ofrece una capacidad de integrar telemetría de forma automática consolidada y correlacionada de hasta 17 marcas y hasta en 29 diferentes productos aprovechando las tecnologías existentes en los ecosistemas de las compañías, dentro de los que puede destacarse AWS, Check Point, Darktrace, Fortinet, Google, Microsoft, Okta, Palo Alto Networks y Rapid 7.

- Sophos NDR— ahora parte de la solución MDR, ofrece protección del tráfico de red para detectar actividades sospechosas que puedan ser un indicativo de actividad de un atacante, combinando técnicas de aprendizaje máquina (ML), analíticos avanzados y técnicas de identificación basado en reglas, detectando un rango más amplio de riesgos incluyendo dispositivos no autorizados, o no protegidos que pudieran ser empleados como punto de entrada. Que, combinado con otra telemetría de Ciberseguridad, habilita a los analistas con una fotografía más compleja de las rutas de ataque y su progresión para habilitar una respuesta más rápida y comprehensiva.

La propuesta de Sophos es la de utilizar toda la información disponible y tecnología avanzada para emprender acciones proactivas y validar contexto de las amenazas de manera que se mitigue, contenga y neutralice amenazas en forma inteligente y más automatizada.

## *Desafíos*

Si bien SOPHOS posee un portafolio amplio de soluciones de Ciberseguridad para cubrir la necesidad de los negocios de asegurar sus ecosistemas extendidos en América Latina, al igual que otros proveedores de Ciberseguridad, puede encontrarse con que algunos clientes no estén preparados para trasladar toda su operación a MDR, debido a la complejidad de las empresas para entender las avanzadas técnicas que emplea el cibercrimen, en muchos casos invisible al ojo inexperto y solo reconocido hasta el momento en que se hace pública una brecha. Por la perspectiva comercial, SOPHOS debe entrenar a su ecosistema de socios y canales sobre el modelo de costos y la forma en que compite contra los modelos tradicionales de MSP, a través de los cuales la compañía puede acercar sus soluciones en América Latina para lograr una mayor penetración del mercado.

## VI. Conclusiones

Es importante conocer los beneficios que cada proveedor de servicios gestionado ofrece y siempre en relación con la necesidad que cubre en cada negocio. También, se debe entender que los servicios gestionados deben ayudar la reducción de la fragmentación tecnológica y su distribución de activos, habilitar el objetivo de construir una postura de ciberseguridad acorde con el apetito de riesgo de la compañía, que permita conocer cuál es el nivel de integración que existe con el *stack* tecnológico de su empresa y evite el *vendor lock-in*; es decir, que permita la integración de servicios o plataformas, aunque no pertenezcan a su marca.

Para IDC, es muy importante recomendar que los servicios deben poder reducir la complejidad que las empresas han creado en sus entornos como la convivencia entre entornos *on-premise, cloud privada, cloud pública*, *multi-cloud*, sistemas legados y las dinámicas de trabajo a distancia.

"El uso de herramientas que mejoren la efectividad de las operaciones, como la reducción de errores humanos, la prevención de la fatiga causada por altos volúmenes de alertas y la reducción de la carga de trabajo repetitivo, en entornos altamente distribuidos, contribuirán a escalar las operaciones al nivel de resiliencia y velocidad que requieren los negocios."

– Emanuel Figueroa.

Es importante impulsar la conciencia de los consumidores para adoptar una postura donde se asuma la brecha, se habiliten procesos de modelado y cacería de amenazas, y empujar fuertemente una cultura centrada en KPIs que busque como objetivo la automatización de tareas.

Además, de contar con el apoyo de un socio tecnológico y de servicios para compartir el tiempo estimado en que la solución genera valor para la compañía, desde la compra hasta la puesta en producción, la contribución a la reducción de la fricción por implementación, configuración y administración de herramientas y cuáles son las eficiencias en costos que permitan tomar una decisión basada en costo-eficiencia.

# Acerca de los Analistas

Emanuel Figueroa, *Analista Senior de Inteligencia de Mercado de Seguridad, Enterprise, IDC Latin America*

Emanuel es analista senior del mercado de seguridad dentro del grupo regional de América Latina. En esta función, se encarga de monitorear y analizar las tendencias y los paisajes competitivos para este mercado, además de desarrollar proyectos de consultoría relacionados con el impacto de las nuevas tecnologías del mercado de seguridad, su panorama y las estimaciones de mercado.

## MENSAJE DEL PATROCINADOR

### Acerca de Sophos Managed Detection and Response (MDR)

Managed Detection and Response (MDR), es un servicio totalmente gestionado prestado por expertos que detectan y responden a ciberataques dirigidos contra su organización las 24 horas del día, 7 días a la semana. Sophos MDR es compatible con una amplia lista de productos de ciber-seguridad de otros fabricantes como: Amazon Web Services (AWS), Check Point, CrowdStrike, Darktrace, Fortinet, Google, Microsoft, Okta, Palo Alto Networks, Rapid7 y muchos más. La telemetría se consolida, se correlaciona y se prioriza automáticamente con información del ecosistema adaptativo de ciber-seguridad de Sophos (ACE) y la inteligencia de amenazas proporcionada por Sophos X-Ops.

Para más información lo invitamos a visitar nuestro sitio:

https://www.sophos.com/es-es/products/managed-detection-and-response.

IDC Custom Solutions

**El contenido de este documento ha sido adaptado a partir de estudios de IDC publicados en www.idc.com.**

**IDC América Latina**
4090 NW 97th Avenue Suite 350,
Doral, FL, USA 33178
+1-305-351-3020
Twitter: @IDCLatin
www.idclatin.com

**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.