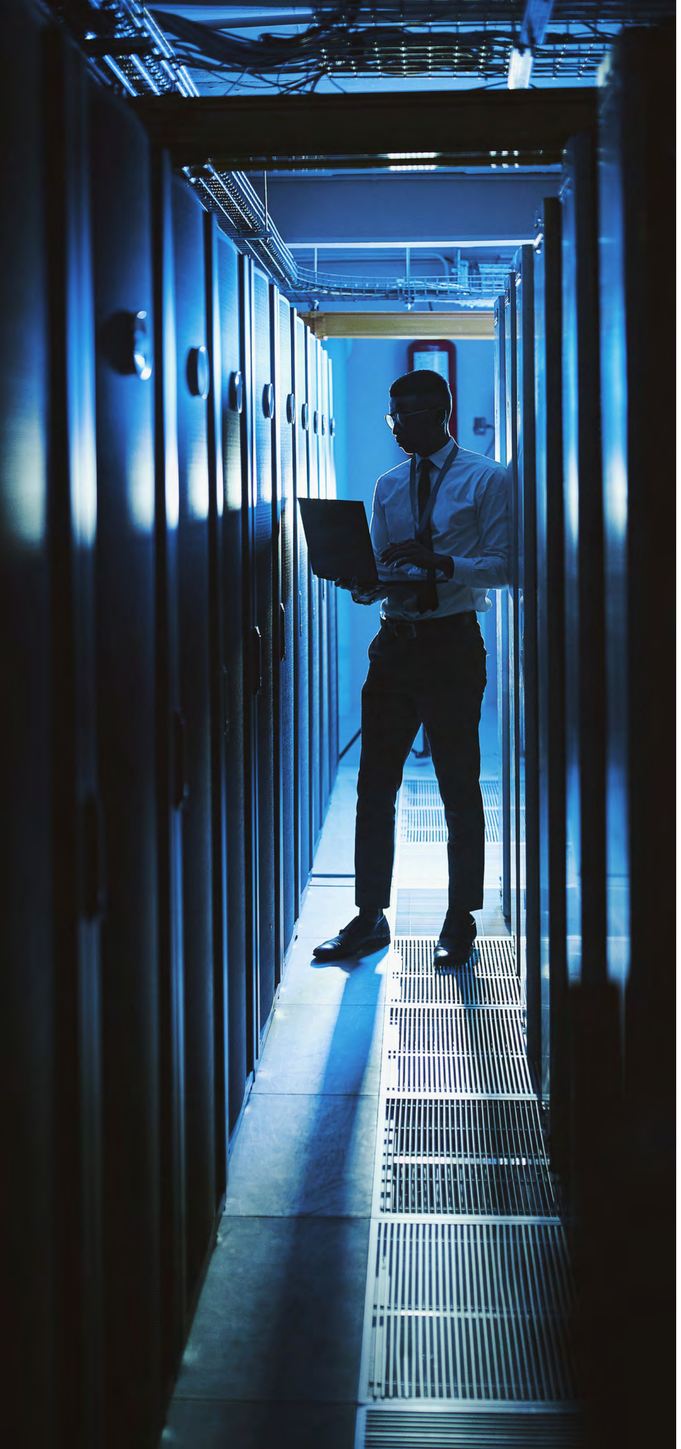
Enterprise Strategy Group | Getting to the bigger truth.™

Lo que los equipos de seguridad desean de los proveedores de MDR

Dave Gruber, analista principal

SEPTIEMBRE DE 2022



Objetivos de la investigación

El uso de servicios de detección y respuesta administradas (MDR) se convirtió en una estrategia estándar en los programas de seguridad modernos. Pero las organizaciones de TI no se deben dejar engañar por el nombre: los proveedores de MDR ofrecen mucho más que detección y respuesta básicas, lo que ayuda a los líderes de TI y seguridad a acelerar el desarrollo de programas y mejorar la postura de seguridad. Con una escasez de habilidades de seguridad cibernética que parece no tener fin, los servicios de MDR pueden poner recursos expertos inmediatos en línea, junto con los mejores procesos y herramientas comprobados en su clase que pueden ayudar a los equipos de seguridad a obtener el control y prepararse para tener éxito en los programas de seguridad del futuro.

A fin de comprender estas tendencias, así como evaluar el estado general de las ofertas de servicio de detección y respuesta administradas, ESG encuestó a 373 profesionales de seguridad cibernética que interactuaban personalmente con la tecnología de seguridad cibernética, incluidos los productos y los servicios, y los procesos.

ESTE ESTUDIO BUSCABA LO SIGUIENTE:

Determinar cómo, dónde y por qué se utilizan los servicios de MDR para apoyar los programas de seguridad.

Obtenga información valiosa sobre lo que más importa para las operaciones de TI, los ejecutivos de líneas de negocios y los usuarios finales.

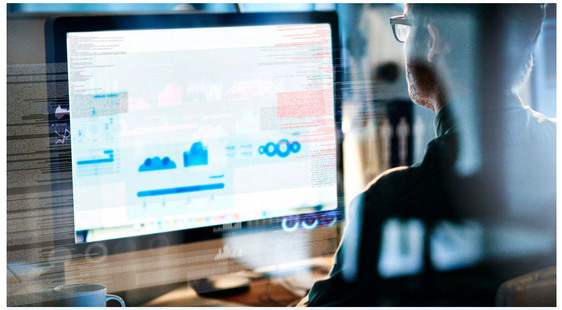
Aísle los casos de uso específicos de MDR y los perfiles organizacionales de aquellos que los utilizan.

Establezca qué megatendencias de la industria influyen en la selección de proveedores de MDR.

VOLVER A CONTENIDO

RESULTADOS CLAVE

HAGA CLIC PARA SEGUIR



Tres factores clave que impulsan la participación inicial de MDR

Las empresas se ven motivadas por evaluaciones proactivas, brechas operacionales y participaciones de respuesta ante incidentes.

Varios casos de uso compatibles con MDR

Los expertos, la inteligencia de amenazas, la formación de habilidades, la cobertura, el desarrollo de programas y más impulsan la participación continua.

MDR impulsa resultados de seguridad positivos

Las empresas notan una madurez avanzada, menos ataques exitosos, habilidades cibernéticas mejoradas y una mayor confianza ejecutiva.

Se espera una pila de tecnología abierta, pero MDR debe incorporar todos los mecanismos

Se espera que los proveedores cuenten con una pila tecnológica completa si es necesario, pero deben integrarse con la infraestructura existente para tener éxito.

Los modelos de participación para clientes de MDR son importantes

Aunque los modelos varían, la confianza se infunde a través de comunicaciones regulares centradas en las personas.

Las megatendencias de la industria influyen en la selección de MDR

El movimiento XDR, la compatibilidad con MITRE ATT&CK y la modernización del SOC son importantes.

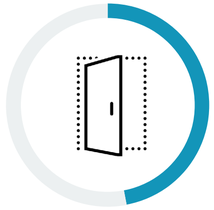
Tres factores clave que impulsan la participación inicial de MDR

Evaluaciones proactivas con más probabilidades de impulsar inicialmente la participación de MDR

¿Qué hace que los equipos de TI y seguridad busquen un proveedor de servicios de detección y respuesta administradas? Si interpretamos MDR de la manera más literal, las brechas en las habilidades, la cobertura o los procesos de las operaciones de seguridad serían una respuesta obvia. Sin embargo, resulta que más de la mitad (57 %) de las empresas mencionó las evaluaciones de seguridad proactivas como un factor que impulsó su participación inicial de MDR. De hecho, las participaciones con proveedores de MDR a menudo comienzan con evaluaciones de seguridad, incluidas las evaluaciones de vulnerabilidades, ya que pueden servir para exponer debilidades en la postura de seguridad en términos de programas, herramientas, cobertura y habilidades. El tercer gran impulsor es una respuesta ante crisis/incidencias que revela las brechas del programa de seguridad. Las necesidades operativas, como la respuesta ante incidentes, también son impulsores comunes de las participaciones de MDR.

Factores que impulsaron las participaciones iniciales con proveedores de MDR.

57 %
Evaluaciones de seguridad

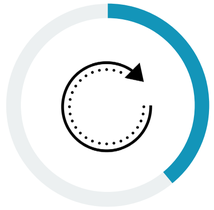


47 %
Evaluación y administración de vulnerabilidades

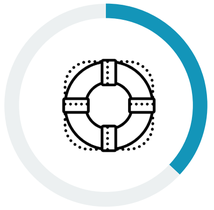
46 %
Servicios de inteligencia de amenazas

39 %
Respuesta ante incidentes/ moderación de incidentes

39 %
Detección de incidentes



39 %
Corrección/recuperación de incidentes



37%
Participación de respuesta ante infracciones o incidentes importantes

36 %
Respuesta ante incidentes de crisis/infracciones que reveló brechas en nuestro programa

34 %
Investigación de incidentes

33 %
Triage y priorización diarias de alertas

30 %
Búsqueda de amenazas

25 %
Formación de equipos rojos y simulación de infracciones y ataques

VOLVER A CONTENIDO

Factores que motivan la participación actual del servicio de MDR

A medida que los equipos de seguridad se esfuerzan por escalar los programas de seguridad para satisfacer el crecimiento y la complejidad de la superficie de ataque y del panorama de amenazas, muchos involucran a proveedores de MDR para acelerar y escalar sus modelos operativos. Las empresas consideran que MDR es una ruta para acelerar el desarrollo de programas y salvar brechas. Más de cuatro de cada diez piensan que los proveedores de servicios de MDR simplemente pueden hacer un mejor trabajo que los recursos internos. Un tercio informa programas de seguridad inmaduros, los que también carecen de las herramientas y los sistemas necesarios. Pero otros impulsores importantes incluyen una lista cada vez mayor de controles y procesos de seguridad necesarios para adquirir seguros de seguridad cibernética, junto con los requisitos de cumplimiento de normas.

Cuando se trata de deficiencias relacionadas con la cobertura y las habilidades, algunas empresas informan brechas, pero estas tienen un rango inferior en la lista en comparación con los objetivos generales de desarrollo y crecimiento de los programas.

Factores que motivan a las empresas a interactuar con sus proveedores de MDR actuales.

VOLVER A CONTENIDO

MDR admite **varios casos de uso**

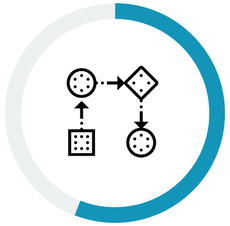
> “Casi la mitad aprovecha un proveedor de MDR **para subcontratar completamente las operaciones de seguridad”.**

Casos de uso clave: Acceso a recursos expertos y al desarrollo de programas de seguridad

Los proveedores de MDR ofrecen una variedad de servicios que se utilizan para satisfacer varios casos de uso. Si bien la aceleración del desarrollo de programas de seguridad y la obtención de acceso a recursos de seguridad expertos lideran la lista, casi la mitad utiliza un proveedor de MDR para subcontratar completamente las operaciones de seguridad. La otra mitad utiliza MDR para complementar su programa interno, cerrar las brechas de cobertura, obtener acceso a inteligencia de amenazas adicional y agregar capacidades de búsqueda de amenazas. También vale la pena señalar que casi la mitad de las empresas subcontratan completamente sus operaciones de seguridad o aspiran a hacerlo.

Casos de uso de MDR dentro de los programas de seguridad de las empresas.

56 %
Acceso a recursos de seguridad expertos

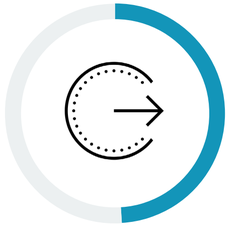


56 %
Desarrollo de programas de seguridad

54 %
Complemento del programa de operaciones de seguridad interno

50 %
Cobertura

50 %
Inteligencia de amenazas



49 %
Subcontratación completa de nuestras operaciones de seguridad

49 %
Búsqueda proactiva de amenazas

VOLVER A CONTENIDO

Las participaciones de MDR suelen crecer con el tiempo

Por lo general, las participaciones de MDR crecen con el tiempo, ya que se agregan nuevos servicios para fortalecer la investigación de incidentes y su moderación y respuesta en caso de que suceda cualquier cosa, desde un evento de crisis o infracción importante hasta actividades de respuesta diarias. Los proveedores de MDR modernos amplían las funcionalidades más allá de las funciones tradicionales, reactivas y estándares de SecOps, ya que ofrecen servicios proactivos que apoyan la inteligencia de amenazas, la búsqueda de amenazas, las simulaciones de ataques, las evaluaciones de seguridad y la administración de vulnerabilidades. En vista de esta amplia recopilación de servicios, los proveedores de MDR ofrecen mucho más que detección y respuesta básicas, ya que se convierten en partners de programas de seguridad a escala completa que ayudan a las empresas de todos los tamaños a escalar sus programas de seguridad.

Se agregaron actividades de seguridad desde la participación inicial con proveedores de MDR.

> Los proveedores de MDR ofrecen **mucho más que detección y respuesta básicas”.**

VOLVER A CONTENIDO

Más que de detección y respuesta: los proveedores de MDR son partners operacionales estratégicos a largo plazo

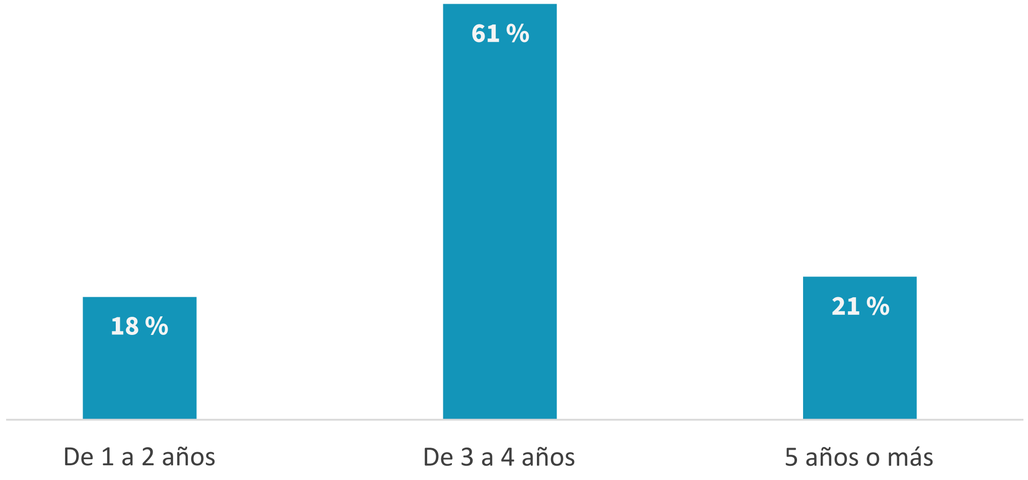
A medida que las participaciones de MDR persistan y las relaciones crezcan, los proveedores de MDR asumirán una función más estratégica. Esto se demuestra claramente por el hecho de que más de tres cuartos (77 %) de las empresas describen a su proveedor de MDR como un partner operativo estratégico en términos de alineación con su programa de seguridad. Estas relaciones persisten, con un 82 % de las empresas que informa la participación de un proveedor de MDR durante al menos tres años, y la mayoría utiliza más de un proveedor de MDR, con un 34 % que se asocia con tres o más proveedores de servicios de MDR para apoyar los casos de uso y los recursos que componen su superficie de ataque.

Lo que las empresas piensan de sus proveedores de MDR actuales.

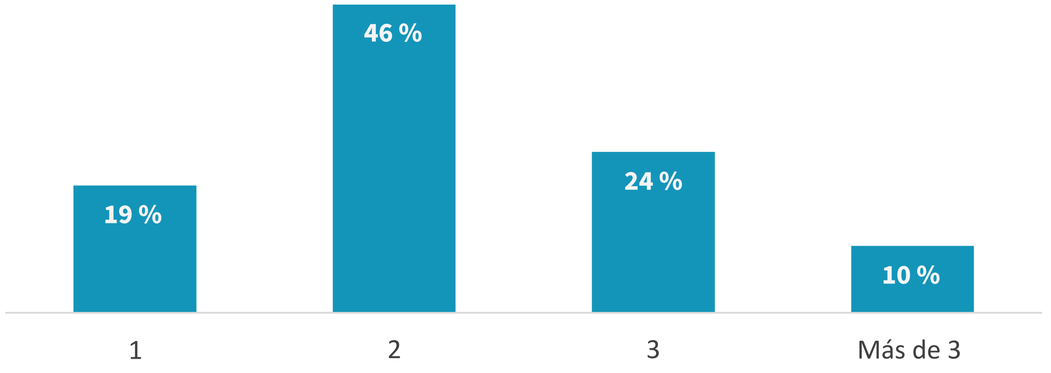
77 %

Un partner operacional estratégico **que mejoró nuestro programa general de seguridad**

Cantidad de tiempo durante la cual las empresas han estado trabajando con un proveedor de MDR.



Cantidad de proveedores de servicios de MDR con los que trabajan las empresas.



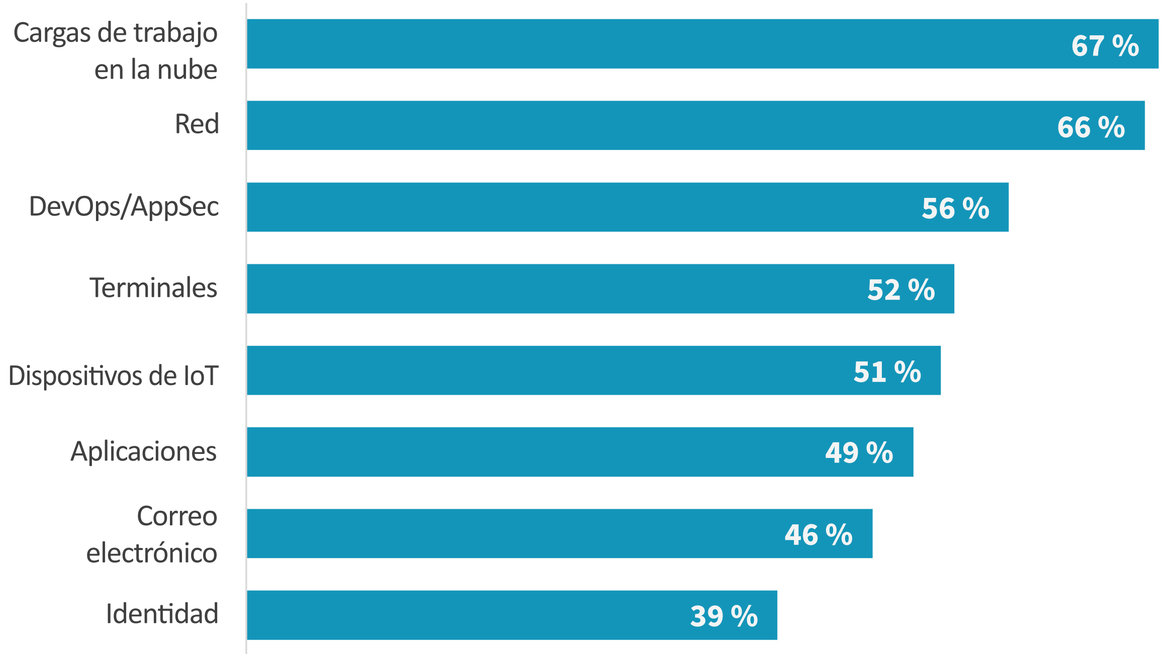
VOLVER A CONTENIDO

> “Pocos recurren a proveedores de MDR **para cubrir toda su superficie de ataque”.**

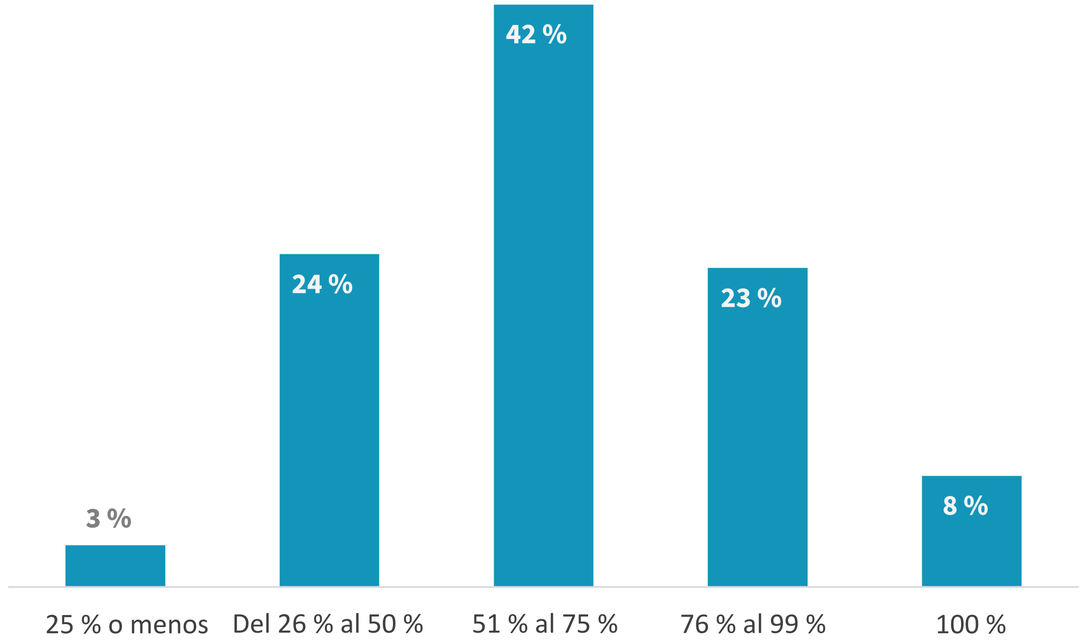
Se espera que los proveedores de MDR supervisen todos los tipos de recursos, pero rara vez el estado completo

Cuando se trata de la cobertura de la superficie de ataque, la mayoría espera que los proveedores de MDR apoyen las operaciones de seguridad para todos los tipos de recursos de TI. Sin embargo, pocos recurren a los proveedores de MDR para cubrir toda su superficie de ataque. Específicamente, más de dos tercios informan que su proveedor de MDR se encarga de cubrir no más del 75 % de su propiedad, mientras que solo el 8 % indica que su proveedor de MDR cubre el 100 %.

Alcance de la cobertura para los proveedores de MDR actuales de las empresas.



Porcentaje de la superficie de ataque que los proveedores de MDR se encargan de cubrir.



VOLVER A CONTENIDO

MDR genera **resultados de seguridad positivos**

Los proveedores de MDR ayudan a mejorar los recursos en el sitio y la madurez de los programas de seguridad

Cuando se trata de los resultados reales alcanzados, los proveedores de MDR ayudan a las empresas a experimentar menos ataques exitosos, acelerar el desarrollo general de los programas de seguridad y abrir oportunidades de inversión en iniciativas de seguridad más estratégicas. Específicamente, la mitad opina que su proveedor de MDR ayuda a mejorar las habilidades de seguridad de sus recursos internos, y el 45 % pudo invertir en iniciativas de seguridad más estratégicas. Más de cuatro de cada diez informan experimentar una cantidad considerablemente menor de ataques exitosos o una mejora general en su programa de seguridad. Desde una perspectiva de línea de negocios, el 42 % señala que la confianza de los ejecutivos o de la junta directiva aumentó, mientras que el 38 % informa que puede cumplir con los objetivos de cumplimiento o los requisitos de seguros cibernéticos. Para confirmar estos resultados positivos del negocio, hubo un aumento significativo en la cantidad de empresas que catalogaron la madurez de sus programas de seguridad como muy madura después de interactuar con un proveedor de MDR.

Resultados obtenidos con la participación de un proveedor de MDR

50 %
Habilidades mejoradas del personal de seguridad aprendidas del proveedor de MDR

45 %
Inversión en iniciativas de seguridad más estratégicas

42 %
Considerablemente menos ataques exitosos

42 %
Mejora significativa del programa de seguridad

42 %
Aumento de la confianza de los ejecutivos o de la junta directiva

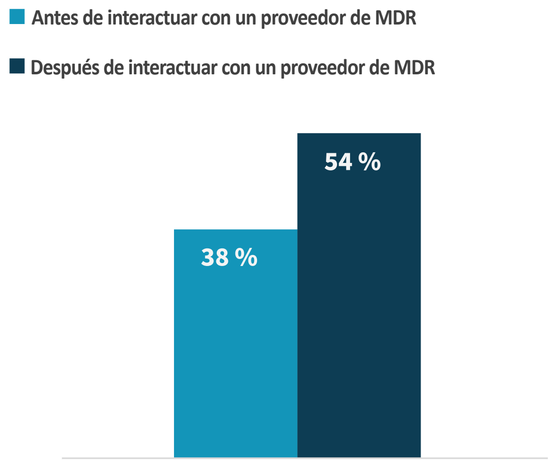
38 %
Seguimiento de los requisitos de cumplimiento/seguro cibernético

38 %
Menores costos de operación de la seguridad

35 %
Menos estrés para el equipo de seguridad interna

32 %
Reducción de las tarifas de seguros cibernéticos

Madurez del programa de MDR.



Muy madura (es decir, procesos formales y operacionalizados, expertos que forman parte del personal, cobertura y visibilidad completas de la superficie de ataque, perfiles de riesgo, programa formal de respuesta ante incidentes ensayado, colaboración de TI, herramientas y análisis de seguridad altamente eficaces, etc.)

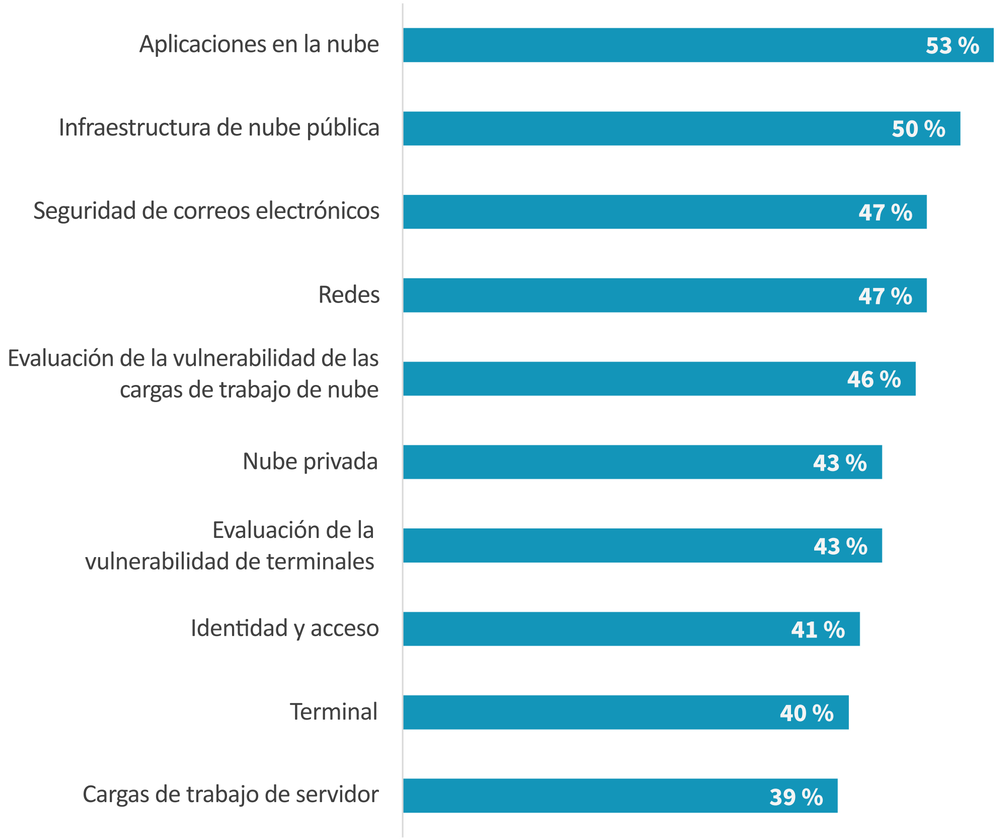
VOLVER A CONTENIDO

Se espera una pila de tecnología abierta, pero **MDR debe incorporar todos los mecanismos**

Las operaciones de nube y de seguridad son criterios tecnológicos clave para la selección de MDR

Los clientes de MDR esperan que su proveedor aparezca con una cobertura de seguridad integral en todos los vectores de ataque. Pero además, los usuarios de MDR esperan que su proveedor trabaje junto con los mecanismos de seguridad ya implementados, los que van desde un conjunto completo de controles de seguridad, incluidos el terminal, la red, la nube y el correo electrónico, hasta una pila completa de herramientas de operaciones de seguridad, incluidas SIEM, SOAR, EDR, NDR, XDR, administración de superficies de ataque, descubrimiento de recursos y administración de vulnerabilidades.

Lo que las empresas de tecnologías de detección/agente esperan de un proveedor de MDR.



Lo que las empresas de tecnologías de operaciones de seguridad esperan de un proveedor de MDR.

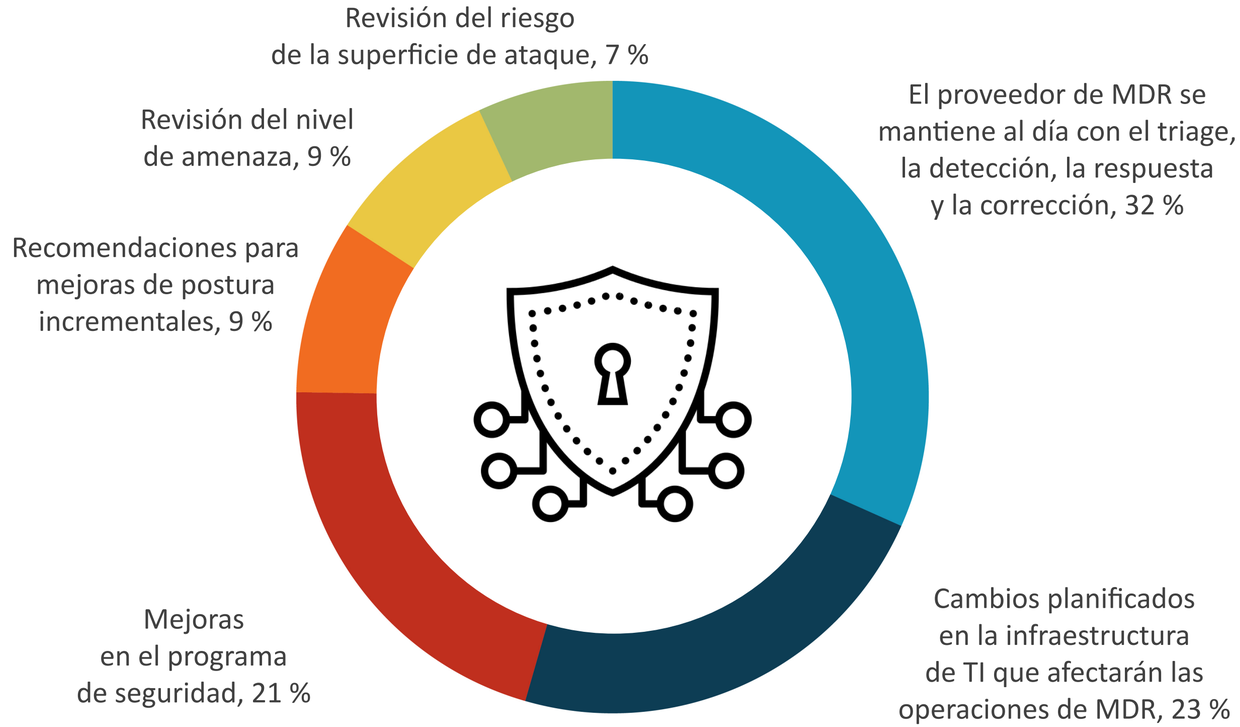
VOLVER A CONTENIDO

Los modelos de participación para clientes de MDR **son importantes**

Revisiones operacionales de MDR: ¿Qué es lo más importante?

Los líderes de seguridad destacan que los modelos de participación de MDR son muy importantes y piden a los proveedores de MDR que además de seguir el ritmo de la detección, respuesta y corrección de su triage, se mantengan al día con los cambios planificados en la infraestructura de TI, las mejoras continuas en los programas de seguridad, la revisión del riesgo de la superficie de ataque y la revisión del nivel de amenazas, todo a la vez que recomiendan acciones para mejorar la postura de seguridad. Estas expectativas son altas, pero demuestran por qué la mayoría de las empresas considera que su proveedor de MDR es un partner estratégico.

Aspecto más importante de los análisis operativos de los proveedores de MDR.



> Los líderes de seguridad destacan que **los modelos de participación de MDR son muy importantes”.**

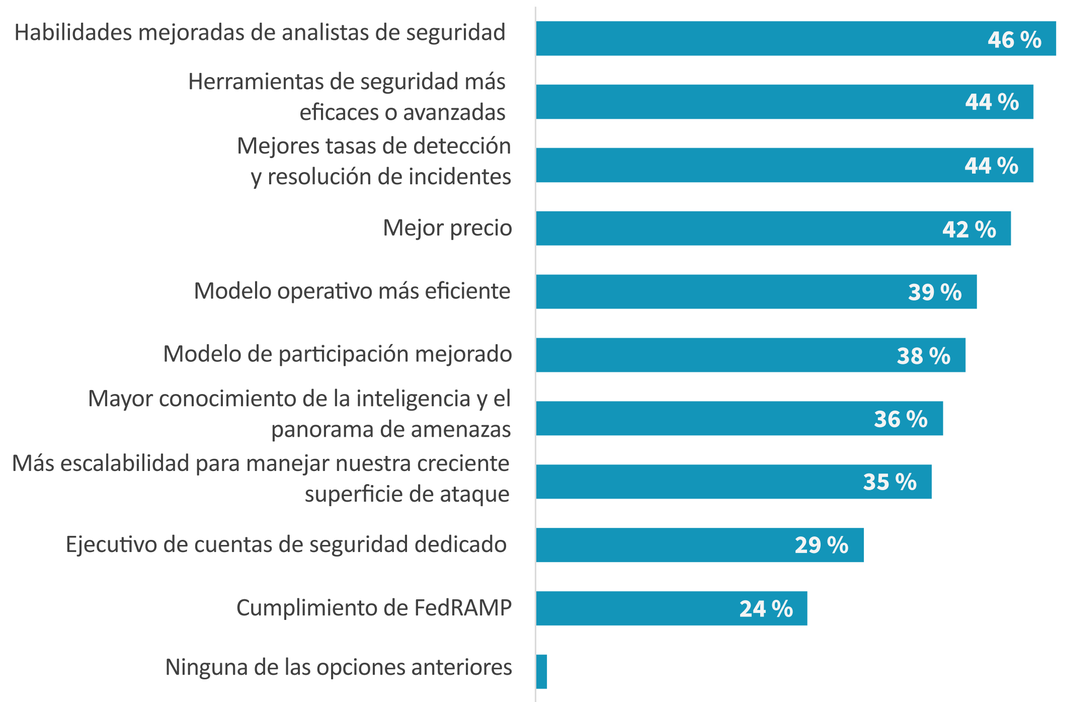
VOLVER A CONTENIDO

Las habilidades y las herramientas avanzadas tienen la capacidad de impulsar el cambio de proveedor de MDR

¿Qué consideraciones son importantes para las empresas cuando evalúan y seleccionan un proveedor de MDR? Casi la mitad (49 %) señaló que debe trabajar con su ecosistema de tecnologías y herramientas de seguridad existente, mientras que el 46 % desea funcionalidades de detección y respuesta avanzadas. Otro 43 % desea que su proveedor de MDR cuente con recursos de seguridad expertos, que es también el factor más mencionado que motivaría a las empresas a cambiar su proveedor actual. Otras razones incluyen herramientas de seguridad más avanzadas y tasas de detección y resolución mejoradas, aunque el precio y los modelos operativos también son importantes.

Criterios de selección importantes para los proveedores de MDR.

Factores que motivarían a las empresas a cambiar los proveedores de MDR.



VOLVER A CONTENIDO

Las megatendencias de la industria **influyen en la selección de MDR**

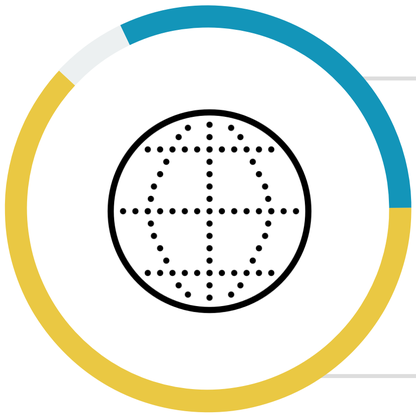
Más de nueve de cada diez

empresas identifican la compatibilidad con MITRE ATT&CK como crítica o muy importante.

La compatibilidad con MITRE y XDR es clave para la mayoría en la selección de proveedores de MDR

La elección de un proveedor de MDR a menudo implica más que una lista de comprobación de las funcionalidades y la cobertura. Los extensos programas de la industria influyen aún más en la selección de proveedores de MDR, y más de nueve de cada diez empresas identifican la compatibilidad con MITRE ATT&CK como crítica (32 %) o muy importante (62 %). Además, casi tres cuartos (73 %) informan que la tecnología de seguridad de detección y respuesta extendidas (XDR) se consideró en el proceso de selección de servicios de MDR. El borde de acceso de servicio seguro (SASE) y la administración de superficie de ataque (ASM) también fueron considerados importantes por dos tercios.

Importancia del proveedor de MDR que cumple con el marco de trabajo MITRE ATT&CK.



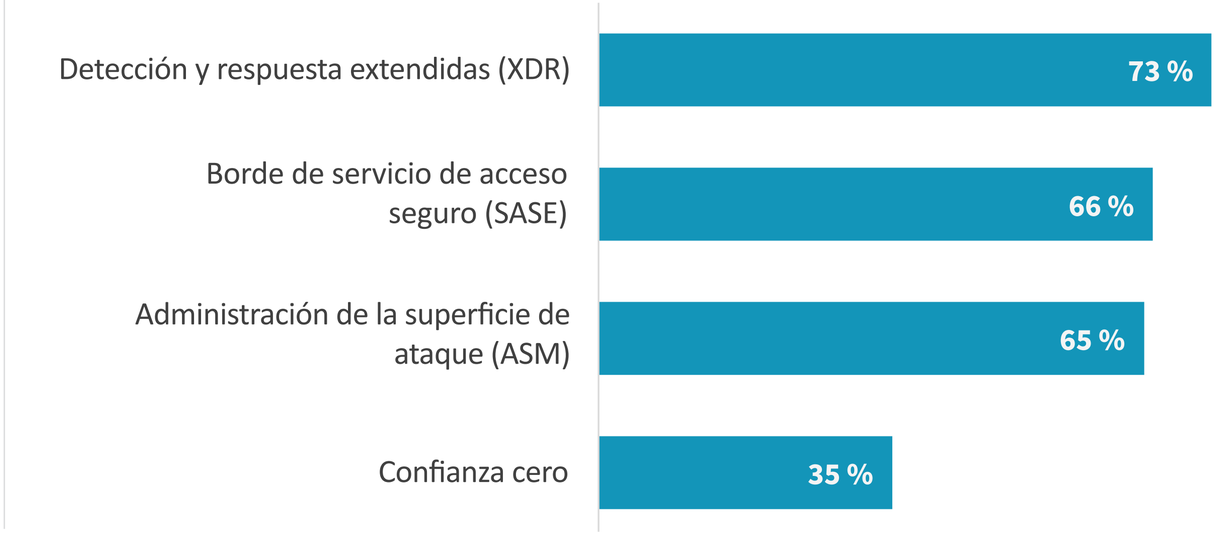
32 %

Crítica: No consideraríamos un proveedor de MDR que no cumpliera con el marco de trabajo MITRE ATT&CK

62 %

Muy importante: Preferimos trabajar con un proveedor de MDR que cumpla con el marco de trabajo MITRE ATT&CK, pero que considere otros

Megatendencias de seguridad consideradas en el proceso de selección de servicios de MDR.



VOLVER A CONTENIDO

MDR se está convirtiendo en una estrategia de seguridad estándar

El uso de servicios de MDR se convirtió en un componente principal de la estrategia de los programas de seguridad, lo que eleva a los proveedores de MDR a la categoría de partners estratégicos. Estos ayudan a los equipos de seguridad y de TI a acelerar el desarrollo de programas, mejorar la postura de seguridad y obtener beneficios menos visibles, como el apoyo de los objetivos de cumplimiento, la adquisición de seguros cibernéticos y la mejora de las habilidades y los procesos de seguridad internos. Por lo tanto, la mayoría considera a MDR como una parte continua de su inversión en programas de seguridad, con un 37 % que informa que MDR es estratégico y crítico, y otro 35 % que planea trabajar con su proveedor de MDR a medida que actualice e implemente estrategias de seguridad futuras.

ESG considera que MDR es una estrategia de seguridad importante y estándar, y recomienda que la empresa explore aún más los casos de uso adicionales que pueden acelerar el desarrollo y la postura de los programas de seguridad.

La función que cumple MDR en el contexto más amplio de la modernización del SOC.

> La mayoría considera a MDR como una **parte continua de su inversión en el programa de seguridad”.**

VOLVER A CONTENIDO

DELL Technologies

Dell Technologies (NYSE: DELL) ayuda a las empresas y a las personas a construir su futuro digital y a transformar la manera en que trabajan, viven y juegan. La empresa proporciona a los clientes el portafolio de tecnología y servicios más amplio e innovador de la industria para la era de los datos.

MÁS INFORMACIÓN

SOBRE ESG

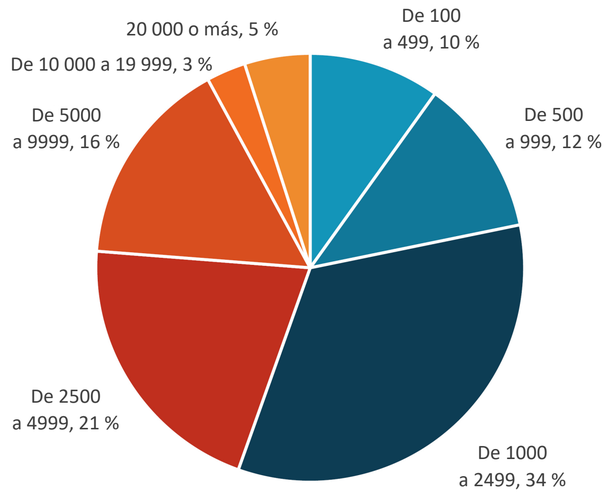
Enterprise Strategy Group es una empresa de estrategia, investigación y análisis integrados de tecnologías que proporciona inteligencia de mercado, información valiosa útil y servicios de contenido de ingreso al mercado a la comunidad tecnológica global.

Metodología de investigación y demografía

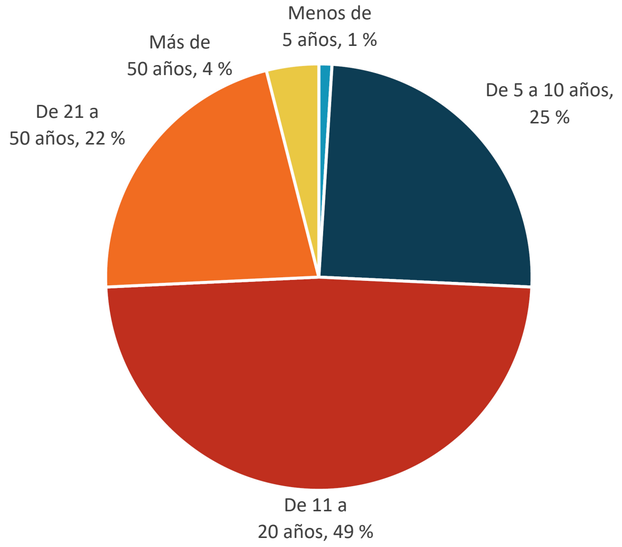
Con el objetivo de recopilar datos para este informe, ESG realizó una encuesta integral en línea a profesionales de seguridad cibernética provenientes de empresas del sector privado y público en Norteamérica (Estados Unidos y Canadá) entre el 3 de agosto de 2022 y el 14 de agosto de 2022. A fin de calificar para esta encuesta, los encuestados debían ser profesionales de seguridad cibernética que estuvieran involucrados personalmente en la tecnología y los procesos de seguridad cibernética, incluidos los productos y los servicios. A todos los encuestados se les proporcionó un incentivo para completar la encuesta en forma de premios en efectivo o equivalentes en efectivo.

Después de filtrar a los encuestados no calificados, eliminar las respuestas duplicadas y analizar las respuestas restantes (según una serie de criterios) para verificar la integridad de los datos, nos quedó una muestra total final de 373 profesionales de seguridad cibernética.

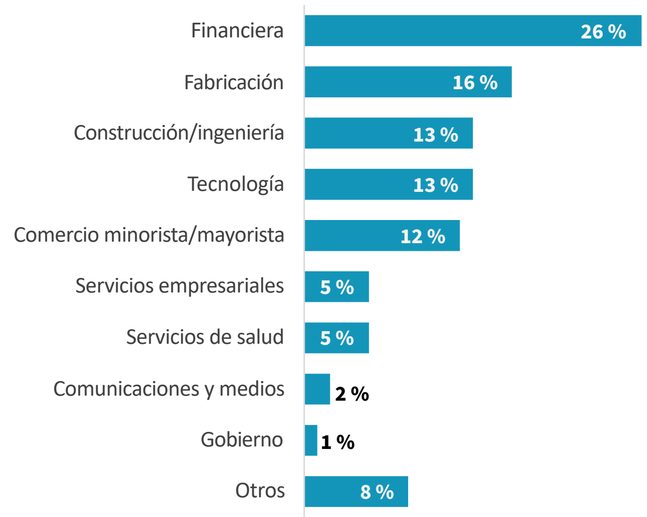
ENCUESTADOS POR CANTIDAD DE EMPLEADOS



ENCUESTADOS POR ANTIGÜEDAD DE LA EMPRESA



ENCUESTADOS POR INDUSTRIA



VOLVER A CONTENIDO

Enterprise Strategy Group es una empresa de estrategia, investigación y análisis integrados de tecnologías que proporciona inteligencia de mercado, información valiosa útil y servicios de contenido de ingreso al mercado a la comunidad tecnológica global.