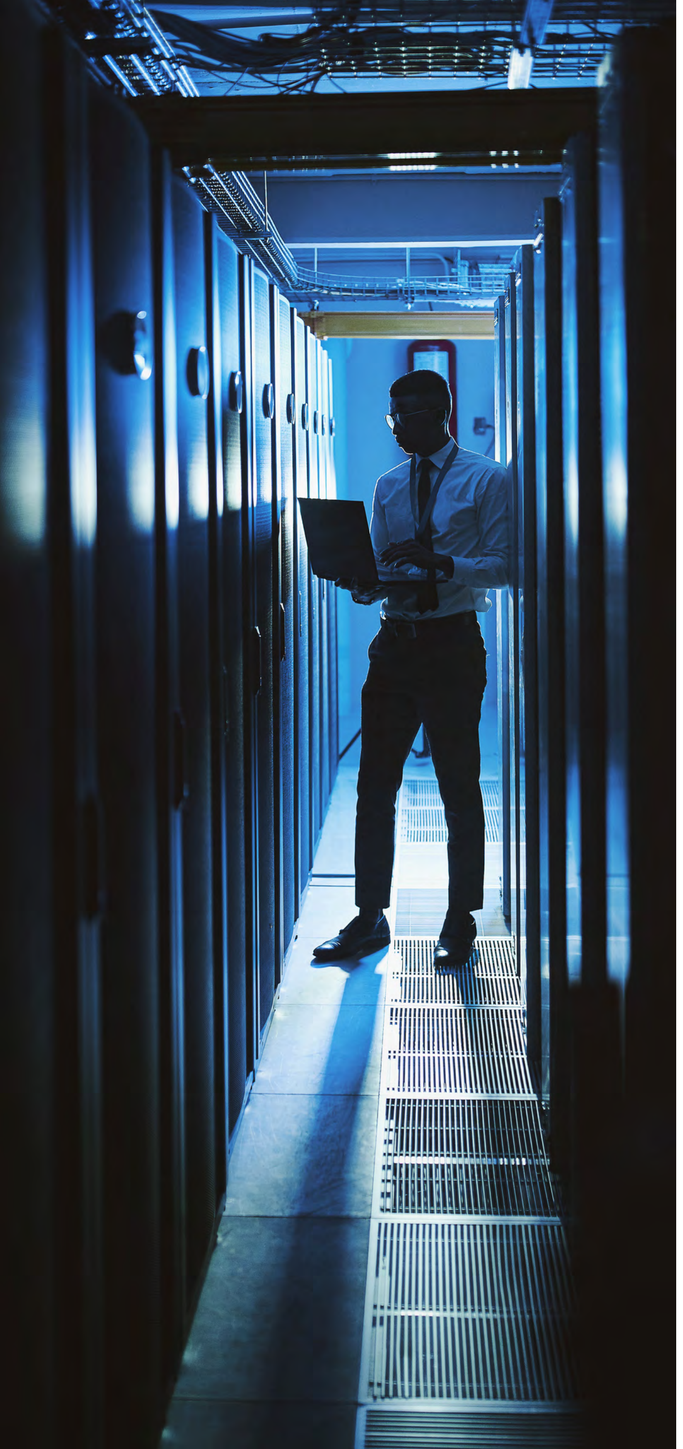
Enterprise Strategy Group | Getting to the bigger truth.™

Qué esperan los equipos de seguridad de los proveedores de MDR

Dave Gruber, Analista principal

SEPTIEMBRE DE 2022



Objetivos de la investigación

Utilizar servicios de detección y respuesta gestionadas (MDR) se ha convertido en una estrategia estándar en los programas de seguridad modernos. No obstante, las organizaciones de TI no deben dejarse engañar por el nombre: los proveedores de MDR ofrecen mucho más que prestaciones de detección y respuesta básicas, también ayudan a los responsables de TI y seguridad a acelerar el desarrollo de programas y a mejorar el estado de seguridad. La falta de profesionales de la ciberseguridad no va a solucionarse en poco tiempo, y los servicios de MDR pueden aportar acceso a expertos en el sitio web de forma inmediata, así como los mejores procesos y herramientas probados, capaces de ayudar a los equipos de seguridad a obtener mayor control y posibilitar el futuro éxito de su programa de seguridad.

A fin de comprender estas tendencias, así como evaluar el estado general de las ofertas de servicios de detección y respuesta gestionadas, ESG encuestó a 373 profesionales de la ciberseguridad involucrados personalmente en la tecnología de ciberseguridad, incluyendo productos, servicios y procesos.

OBJETIVOS DEL ESTUDIO:

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

Obtener información sobre lo que más importa a los equipos de operaciones de TI, los ejecutivos de LOB y los usuarios finales.

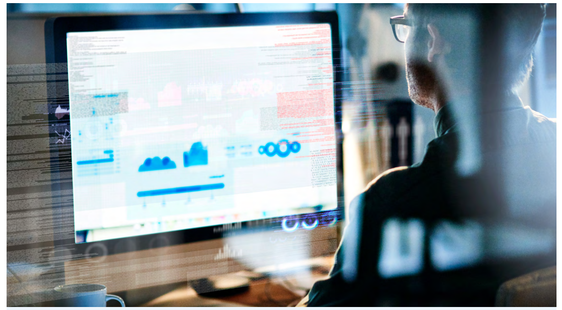
Determinar los casos de uso específicos de las MDR y el perfil organizativo de quienes las utilizan.

Identificar qué grandes tendencias del sector repercuten en la selección de proveedores de MDR.

VOLVER AL ÍNDICE

RESULTA-DOS **CLAVE**

HAGA CLIC PARA ACCEDER



Tres factores clave impulsan el contacto inicial con la MDR

Las organizaciones actúan tras las evaluaciones proactivas, las brechas operativas y la participación del equipo de relaciones con los inversores (IR).

La MDR respalda varios casos de uso

Los casos de uso de expertos, inteligencia contra amenazas, cobertura y desarrollo de programas, entre otros, impulsan la interacción continua.

MDR hace realidad resultados de seguridad positivos

Las organizaciones disfrutan de mayor madurez, menos ataques perpetrados con éxito, mejora en los conocimientos de ciberseguridad y un aumento en la confianza de los ejecutivos.

Se espera que los proveedores de MDR cuenten con una pila de tecnología abierta, pero deben aportar todos los mecanismos

Se espera que los proveedores dispongan de una pila completa si fuese necesario, pero deben integrarse con la infraestructura existente para alcanzar el éxito.

Los modelos de interacción con el cliente de MDR son importantes

Si bien los modelos varían, la confianza se desarrolla mediante comunicaciones periódicas de una persona a otra.

Las grandes tendencias del sector afectan la selección de MDR

La tendencia de la XDR, la compatibilidad con MITRE ATT&CK y la modernización del centro de operaciones de seguridad (SOC) son importantes.

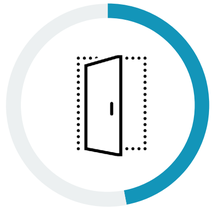
Tres factores clave que impulsan el contacto inicial con la MDR

Las evaluaciones proactivas tienen más probabilidades de impulsar el contacto inicial con la MDR

¿Qué lleva a los equipos de TI y seguridad a buscar un proveedor de servicios de detección y respuesta gestionadas? La respuesta obvia sería la idea de la MDR en su encarnación más literal, las brechas en los conocimientos de seguridad de operaciones, la cobertura o los procesos. No obstante, resulta que más de la mitad (57 %) de las organizaciones nombraron una evaluación de la seguridad proactiva como factor que impulsó el contacto inicial con la MDR. De hecho, el contacto con los proveedores de MDR suele empezar por las evaluaciones de seguridad (incluyendo la evaluación de vulnerabilidades), que pueden destapar debilidades en el estado de seguridad relacionadas con programas, herramientas, cobertura y conocimientos. El tercer gran factor impulsar es una crisis o una respuesta a un incidente que revelen carencias en el programa de seguridad. Las necesidades operativas, como la respuesta ante incidentes, también suelen ser factores impulsores del contacto con la MDR.

Factores que impulsaron el contacto inicial con proveedores de MDR:

57 %
Evaluaciones de seguridad

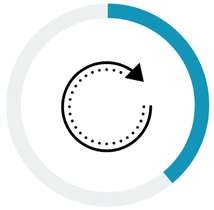


47 %
Evaluación y gestión de vulnerabilidades

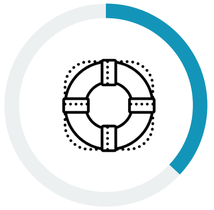
46 %
Servicios de inteligencia contra amenazas

39 %
Respuesta o mitigación de incidentes

39 %
Detección de incidentes



39 %
Corrección y recuperación ante incidentes



37 %
Contacto como respuesta ante una vulneración o un incidente grave

36 %
Respuesta ante una crisis o un incidente causados por una vulnerabilidad que reveló carencias en el programa

34 %
Investigación de incidentes

33 %
Priorización de alertas y triage diarios

30 %
Persecución de amenazas

25 %
Prácticas de equipo rojo o simulaciones de vulneraciones y ataques

VOLVER AL ÍNDICE

Factores que motivan a las organizaciones a colaborar con sus proveedores de MDR actuales

Los equipos de seguridad tienen dificultades para ampliar los programas de seguridad de forma que aborden el crecimiento y la complejidad de la superficie de ataque y el panorama de amenazas, y muchos recurren a proveedores de MDR para acelerar y ampliar sus modelos operativos. Las organizaciones ven la MDR como un método para acelerar el desarrollo de programas y solventar las carencias. Más de 4 de cada 10 piensan que, sencillamente, los proveedores de servicios de MDR son más eficaces que los recursos locales. Un tercio cita los programas de seguridad poco maduros, así como la falta de herramientas y sistemas necesarios. Pero existen otros factores desencadenantes importantes, como las listas cada vez más largas de controles y procesos de seguridad necesarios para adquirir un seguro de ciberseguridad, así como los requisitos de cumplimiento de normas.

Algunos encuestados mencionan carencias de conocimientos y cobertura, pero ocupan un lugar poco prominente en la lista en comparación con el crecimiento general de los programas y los objetivos de desarrollo.

Factores que motivan a las organizaciones a colaborar con sus proveedores de MDR actuales:

VOLVER AL ÍNDICE

MDR admite **múltiples casos de uso**

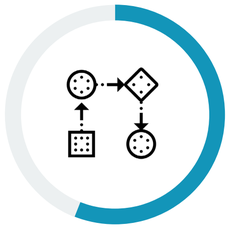
> “Casi la mitad recurren a proveedores de MDR **para subcontratar por completo las operaciones de seguridad”.**

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

Los proveedores de MDR ofrecen una gama de servicios que se utilizan para abordar múltiples casos de uso. Aunque acelerar el desarrollo de programas de seguridad y acceder a expertos en seguridad están a la cabeza de la lista, casi la mitad recurren a proveedores de MDR para subcontratar por completo las operaciones de seguridad. La otra mitad utiliza MDR para complementar su programa interno y zanjar brechas en la cobertura, obtener acceso a inteligencia contra amenazas adicional y obtener prestaciones de persecución de amenazas. También cabe destacar que casi la mitad de las organizaciones subcontratan por completo la seguridad o aspiran a lograrlo.

Casos de uso de la MDR en las organizaciones con programas de seguridad:

56 %
Acceso a expertos en seguridad

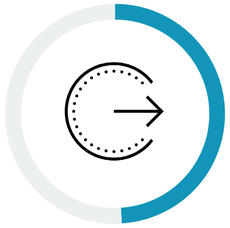


56 %
Desarrollo de programas de seguridad

54 %
Complemento para el programa interno de operaciones de seguridad

50 %
Cobertura

50 %
Inteligencia contra amenazas



49 %
Subcontratación de todas nuestras operaciones de seguridad

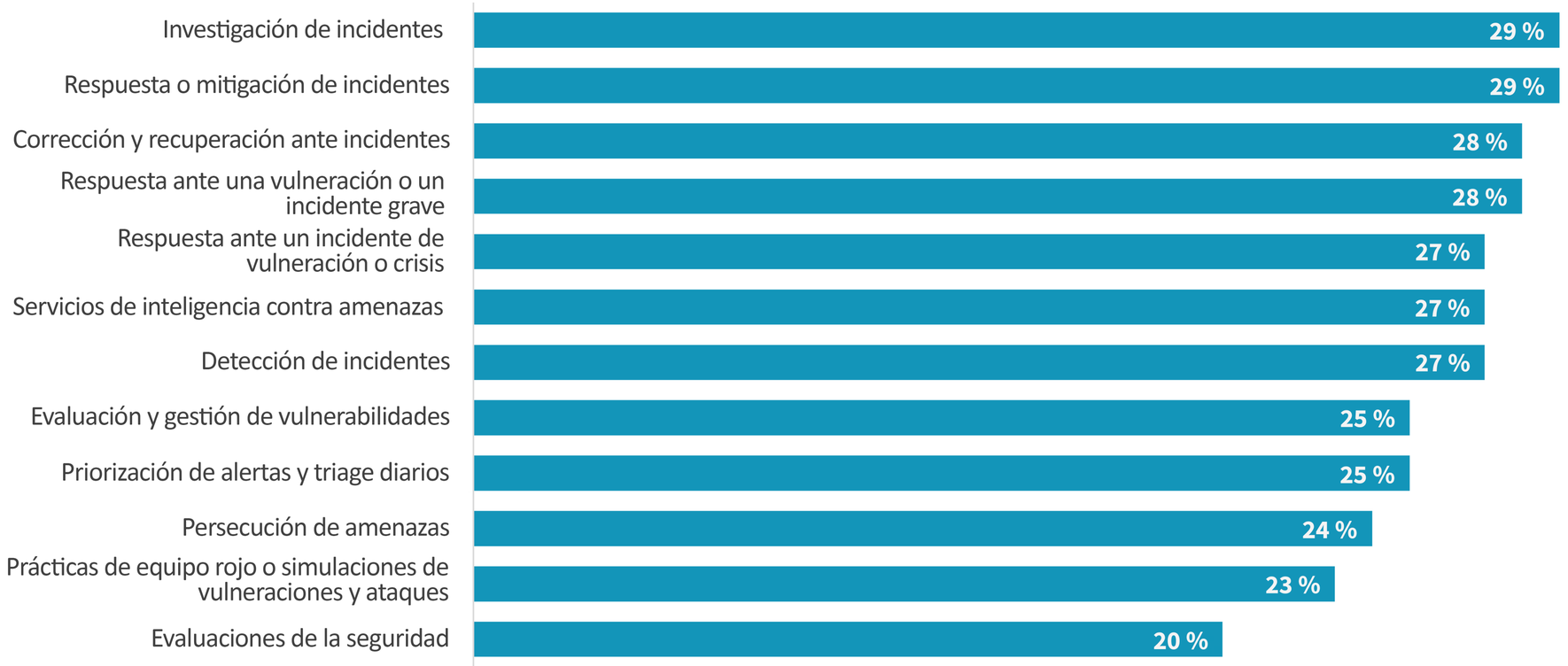
49 %
Persecución proactiva de amenazas

VOLVER AL ÍNDICE

El uso de MDR suele aumentar a lo largo del tiempo

El uso de MDR suele aumentar a lo largo del tiempo; es habitual añadir nuevos servicios para reforzar la investigación, mitigación y respuesta ante incidentes, ya sean grandes crisis o vulneraciones, o actividades diarias de respuesta. Los proveedores de MDR amplían sus prestaciones más allá de las tradicionales funciones reactivas de SecOps estándar, y ofrecen servicios proactivos para respaldar la inteligencia contra amenazas, la persecución de amenazas, las simulaciones de ataques, las evaluaciones de la seguridad y la gestión de vulnerabilidades. Si observamos esta amplia colección de servicios, los proveedores de MDR aportan mucho más que funciones básicas de detección y respuesta, y se están convirtiendo en socios del programa de seguridad por derecho propio, que ayudan a organizaciones de todos los tamaños a ampliar sus programas de seguridad.

Actividades de seguridad añadidas desde el contacto inicial con proveedores de MDR:



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

VOLVER AL ÍNDICE

Más que detección y respuesta: los proveedores de MDR son socios de operaciones estratégicos y a largo plazo

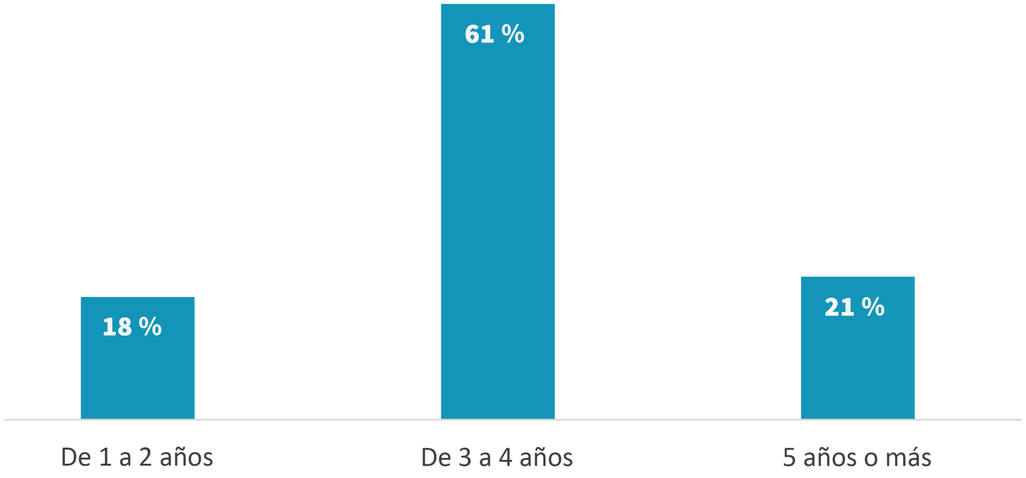
A medida que continua la colaboración alrededor de la MDR y las relaciones se desarrollan, los proveedores de MDR adoptan un papel más estratégico. Esto queda claramente demostrado por el hecho de que más de tres cuartos de las organizaciones (77 %) describen a sus proveedores de MDR como un socio operativo estratégico en lo relativo a la coordinación con su programa de seguridad. Estas colaboraciones son duraderas. El 82 % de las organizaciones afirman que llevan colaborando con un proveedor de MDR desde hace al menos 3 años; la mayoría colaboran con más de un proveedor de MDR, con un 34 % colaborando con 3 o más proveedores de servicios de MDR a fin de respaldar los casos de uso y recursos que conforman su superficie de ataque.

Cómo ven las organizaciones a sus actuales proveedores de MDR.

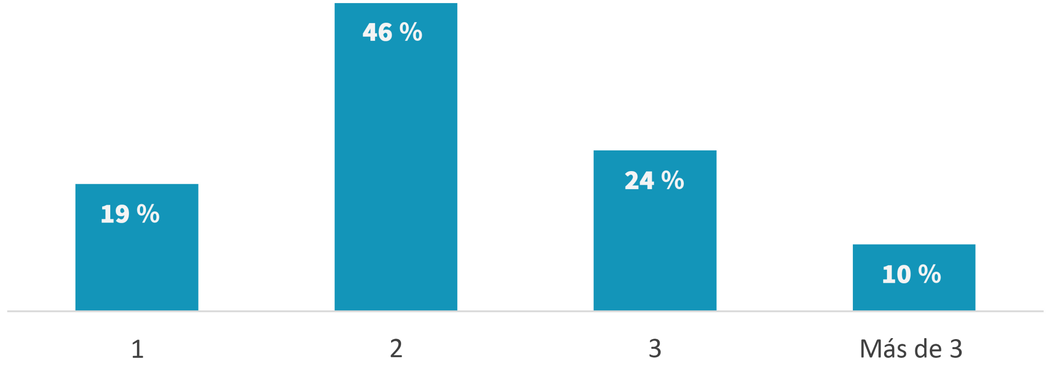
77 %

Un socio operativo estratégico **que ha mejorado nuestro programa de seguridad en general**

Duración de la colaboración entre la organización y un proveedor de MDR:



Cantidad de proveedores de servicios de MDR con los que colaboran las organizaciones:



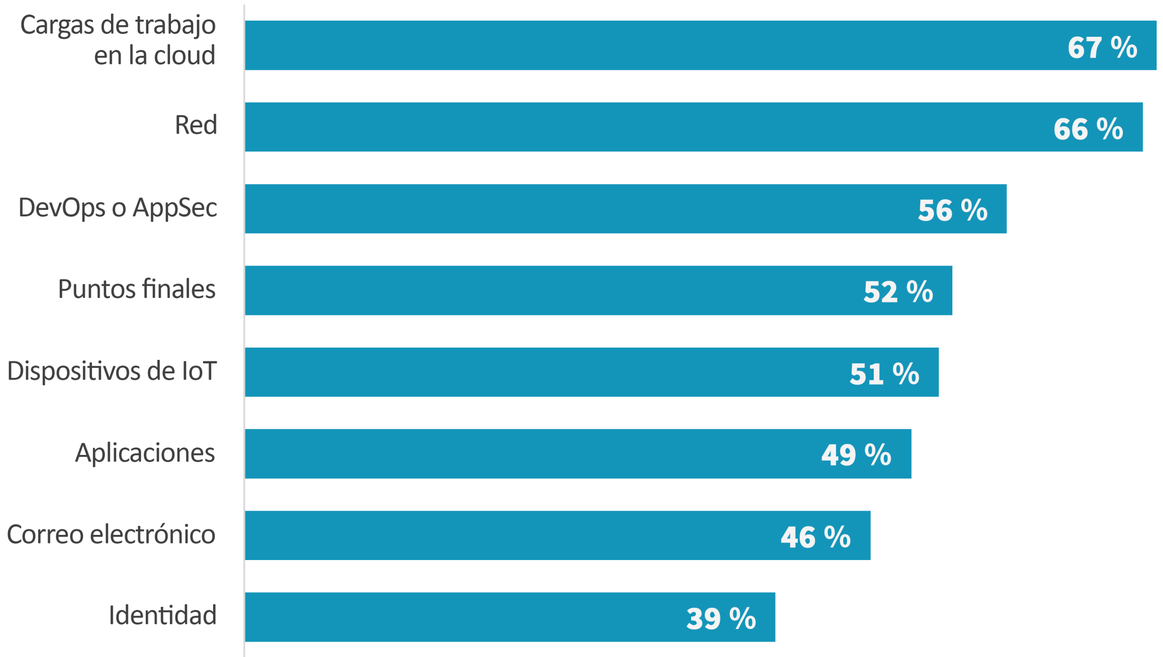
VOLVER AL ÍNDICE

> “Pocas organizaciones colaboran con proveedores de MDR **para cubrir toda la superficie de ataque”.**

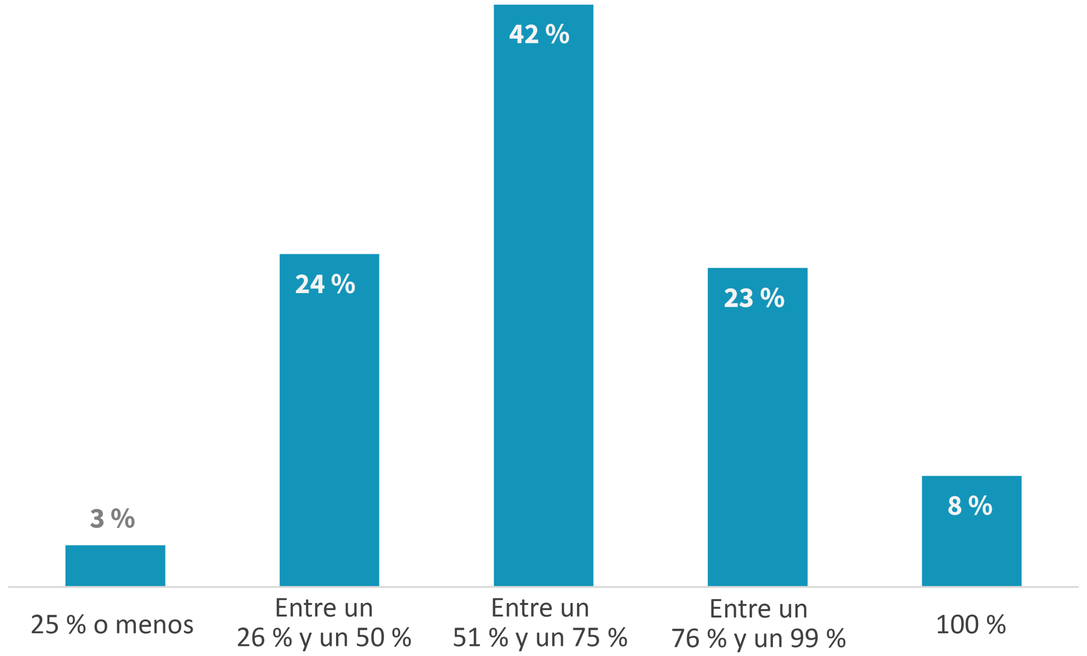
Se espera que los proveedores de MDR supervisen todo tipo de recursos, pero raramente todo el entorno informático

Al hablar de cobertura de la superficie de ataque, la mayoría espera que los proveedores de MDR respalden operaciones de seguridad para todo tipo de recursos de TI. No obstante, pocas organizaciones colaboran con proveedores de MDR para cubrir toda la superficie de ataque. En concreto, más de dos tercios informan de que su proveedor de MDR es responsable de cubrir un máximo de 75 % del entorno informático, y solo el 8 % afirman que un proveedor de MDR cubre el 100 % del entorno.

alcance de la cobertura de los proveedores de MDR actuales en las organizaciones:



Porcentaje de la superficie de ataque que se espera que cubran los proveedores de MDR:



VOLVER AL ÍNDICE

La MDR impulsa **resultados de seguridad positivos**

Los proveedores de MDR ayudan a mejorar los recursos locales y la madurez del programa de seguridad

En lo relativo a los resultados reales obtenidos, los proveedores de MDR ayudan a las organizaciones a sufrir menos ataques perpetrados con éxito, acelerar el desarrollo general del programa de seguridad y acceder a oportunidades de inversión en iniciativas de seguridad más estratégicas. En concreto, la mitad de los encuestados afirman que su proveedor de MDR les ayuda a mejorar los conocimientos sobre seguridad de los recursos internos, y el 45 % han podido invertir más en iniciativas de seguridad más estratégicas. Más de 4 de cada 10 afirman que hubo una cantidad significativamente menor de ataques perpetrados con éxito, así como una mejora general en el programa de seguridad. Desde el punto de vista de las líneas de negocio, el 42 % afirman que ha aumentado la confianza de los ejecutivos y las juntas directivas, y un 38 % afirman poder cumplir los objetivos de cumplimiento normativo o los requisitos para los seguros cibernéticos. Corroborando estos resultados empresariales positivos, hubo un aumento significativo en la cantidad de organizaciones que describen la madurez de su programa de seguridad como “muy maduro” tras colaborar con un proveedor de MDR.

Resultados obtenidos tras colaborar con un proveedor de MDR:

50 %
Mejora en los conocimientos del personal de seguridad gracias a la información proporcionada por el proveedor de MDR

45 %
Inversión en iniciativas de seguridad más estratégicas

42 %
Reducción significativa en la cantidad de ataques perpetrados con éxito

42 %
Mejora significativa en el programa de seguridad

42 %
Mayor confianza entre los ejecutivos y la junta directiva

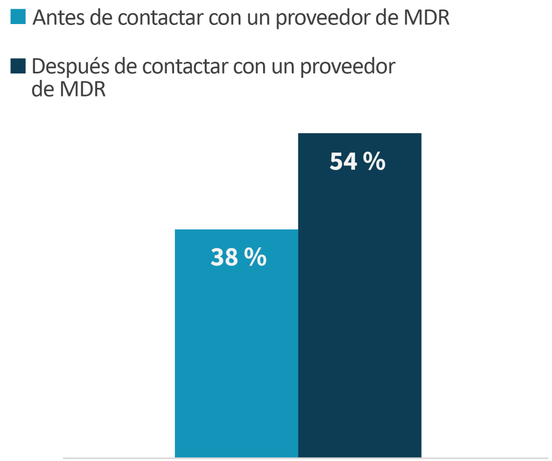
38 %
Cumplimiento normativo y de los requisitos para los seguros cibernéticos

38 %
Menos costes operativos de seguridad

35 %
Reducción del estrés del equipo de seguridad interno

32 %
Disminución de los costes del seguro cibernético

Madurez del programa de MDR:



Muy maduro (es decir, procesos formales u operacionalizados, personal experto, cobertura y visibilidad completas de la superficie de ataque, perfiles de riesgo, programa de IR formal y probado, colaboración de TI, herramientas y análisis de seguridad muy eficaces, etc.).

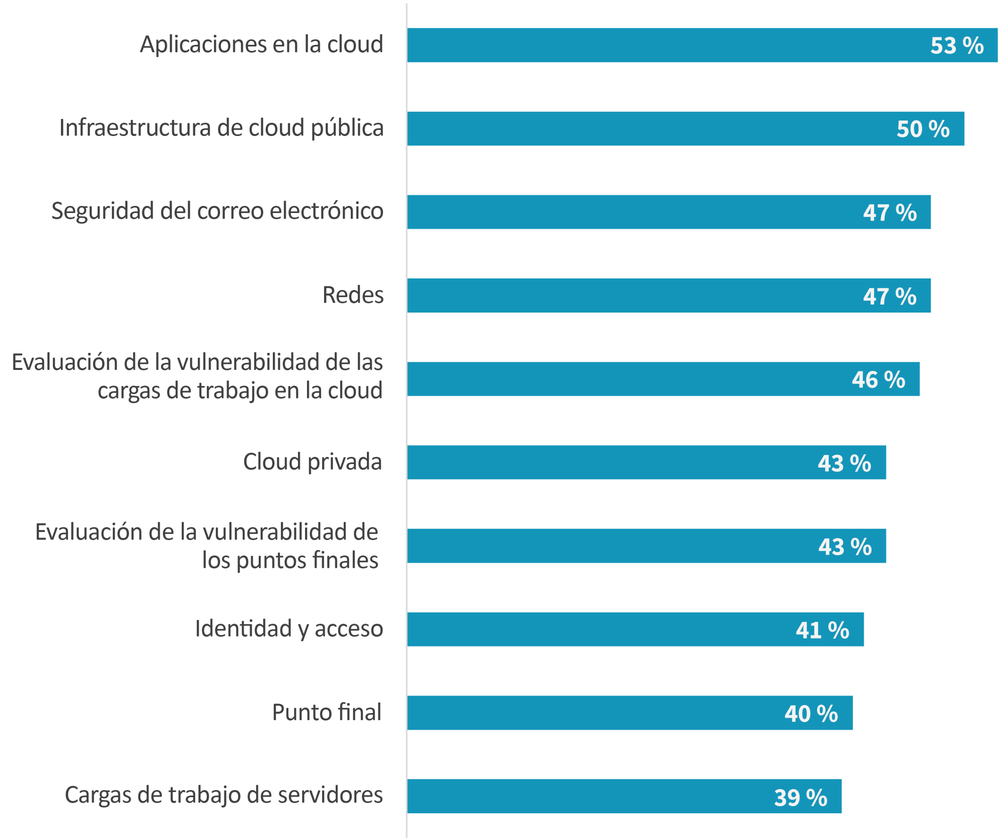
VOLVER AL ÍNDICE

Se espera que los proveedores de MDR cuenten con una pila de tecnología abierta,**pero deben aportar todos los mecanismos**

Las operaciones de cloud y seguridad son un criterio tecnológico clave para la elección de MDR

Los clientes de MDR esperan que los proveedores cuenten con una cobertura de seguridad completa, que abarque todos los vectores de seguridad. Además, los usuarios de MDR esperan que el proveedor pueda trabajar con los mecanismos de seguridad de los que ya disponen; que pueden abarcar desde controles de seguridad completos (incluyendo puntos finales, redes, cloud y correo electrónico), hasta una pila completa de herramientas de operaciones de seguridad (incluyendo SIEM, SOAR, EDR, NDR, XDR, gestión de la superficie de ataque, identificación de recursos y gestión de vulnerabilidades).

Tecnologías de identificación y agentes que las organizaciones esperan de un proveedor de MDR:



Tecnologías de operaciones de seguridad que las organizaciones esperan de un proveedor de MDR:

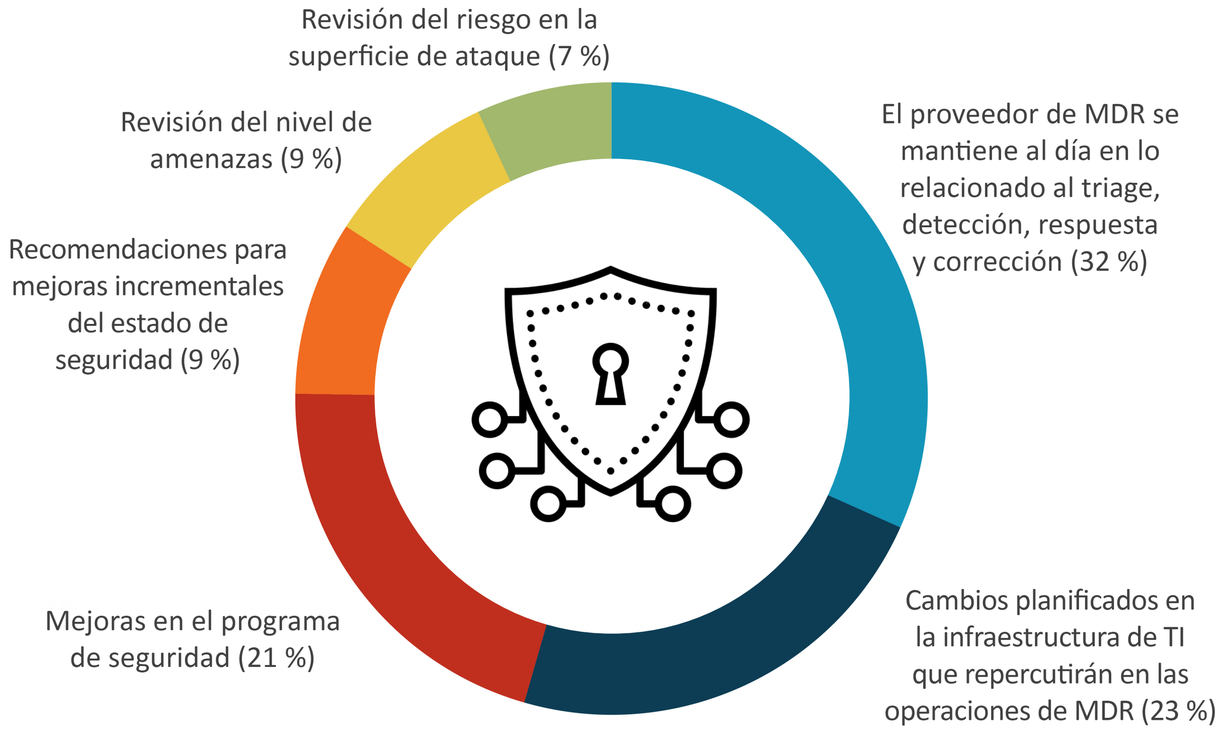
VOLVER AL ÍNDICE

Los modelos de interacción con el cliente de MDR **son importantes**

Revisiones operativas de MDR: lo más importante

Los responsables de seguridad hacen hincapié en que los modelos de interacción de MDR son muy importantes, y piden a los proveedores de MDR no solo que mantengan el triage y la detección, la respuesta y la corrección; sino también que se mantengan al día de los cambios planificados en la infraestructura de TI y que ofrezcan mejoras continuas para el programa de seguridad, una revisión de los riesgos de la superficie de ataque y revisión del nivel de riesgo; todo ello al tiempo que recomiendan acciones para continuar mejorando estado de seguridad. Se trata de expectativas altas, pero demuestran por qué la mayoría de las organizaciones considerar a los proveedores de MDR socios estratégicos.

Aspectos más importantes de las revisiones operativas de los proveedores de MDR:



> Los responsables de seguridad hacen hincapié en que los **modelos de interacción de MDR son muy importantes”.**

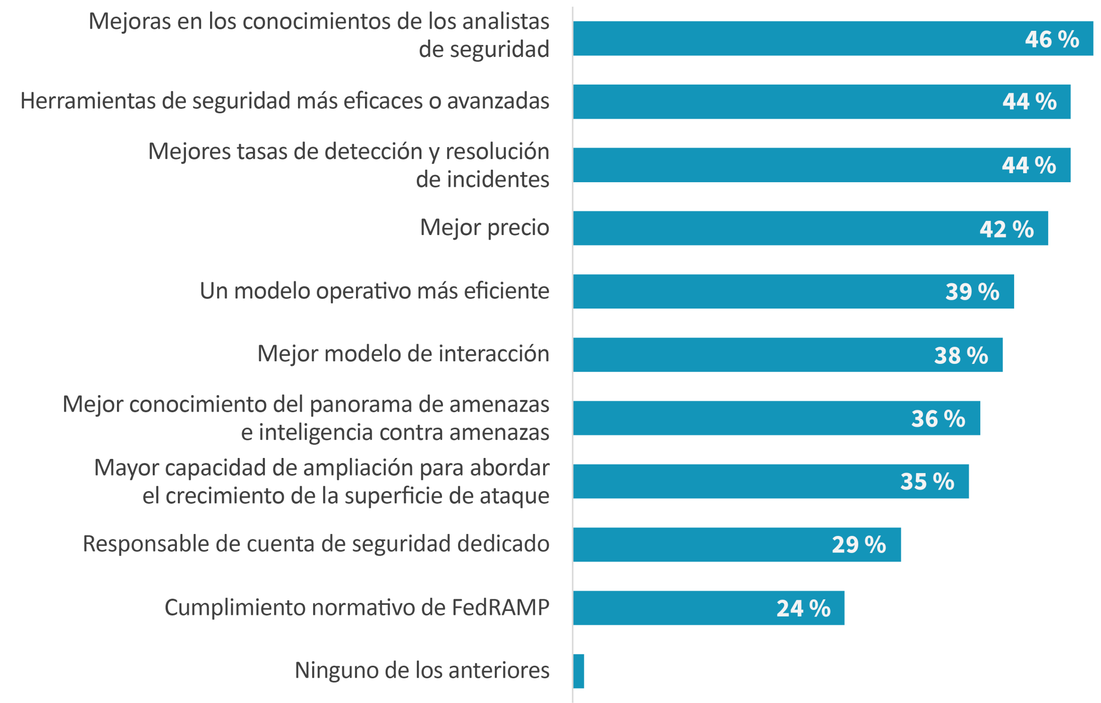
VOLVER AL ÍNDICE

Las herramientas y los conocimientos avanzados son capaces de impulsar un cambio de proveedor de MDR

¿Qué consideraciones resultan importantes para las organizaciones al evaluar y elegir un proveedor de MDR? Casi la mitad (49 %) afirmaron que deben poder trabajar con su ecosistema existente de herramientas y tecnologías de seguridad; y un 46 % quieren que dispongan de prestaciones avanzadas de detección y respuesta. Un 43 % más quieren que los proveedores de MDR cuenten con recursos de seguridad expertos, lo que también es el factor que se mencionó más como motivo para que una organización cambie de proveedor. Otros motivos son herramientas de seguridad más avanzadas y mejoras en la tasa de detección y corrección, aunque los precios y los modelos operativos también importan.

Criterios importantes para la elección de proveedores de MDR:

Factores que motivarían a las organizaciones a cambiar de proveedor de MDR:



VOLVER AL ÍNDICE

Las grandes tendencias en el sector **repercuten en la elección de MDR**

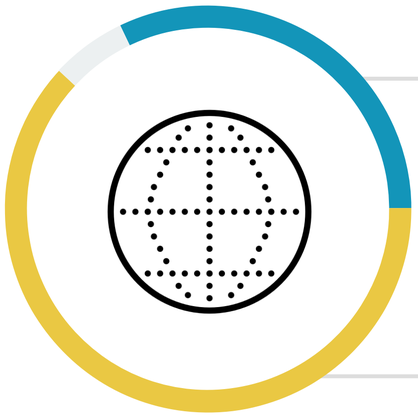
Más de 9 de cada 10

organizaciones describen la compatibilidad con MITRE ATT&CK como “crítica” o “muy importante”.

La compatibilidad con MITRE y XDR son fundamentales para la mayoría al elegir un proveedor de MDR

Elegir un proveedor de MDR suele consistir en algo más que una lista de capacidades y cobertura. Los grandes programas dentro del sector repercuten en la elección de proveedores de MDR, y más de 9 de cada 10 organizaciones afirman que la compatibilidad con MITRE ATT&CK es crítica (32 %) o muy importante (62 %). Además, casi tres cuartas partes (73 %) afirmas que la tecnología de seguridad de detección y respuesta ampliadas (XDR) se tuvo en cuenta durante el proceso de selección de los servicios MDR. Dos tercios de los encuestados también consideraron importantes el perímetro de servicio de acceso seguro (SASE) y la gestión de la superficie de ataque (ASM).

Importancia de que el proveedor de MDR ofrezca compatibilidad con el marco de referencia de MITRE ATT&CK:



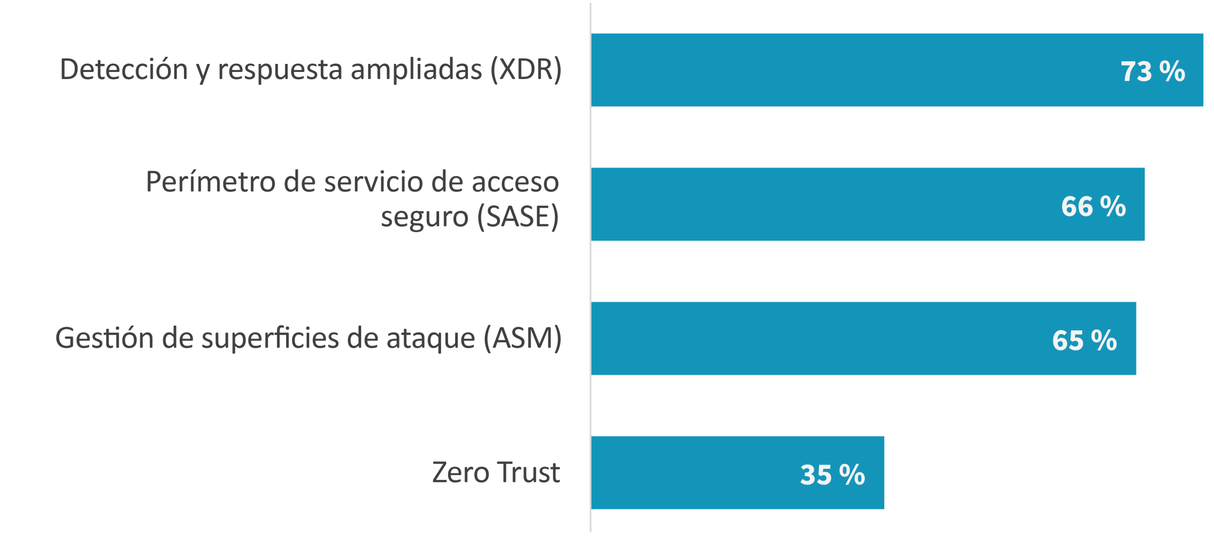
32 %

Crítica: descartaríamos cualquier proveedor de MDR que no ofreciera compatibilidad con el marco de referencia de MITRE ATT&CK.

62 %

Muy importante: preferimos colaborar con un proveedor de MDR que ofrezca compatibilidad con el marco de referencia de MITRE ATT&CK, pero tendríamos en cuenta a los que no lo hicieran.

Grandes tendencias en seguridad que se tuvieron en cuenta durante el proceso de selección de los servicios de MDR:



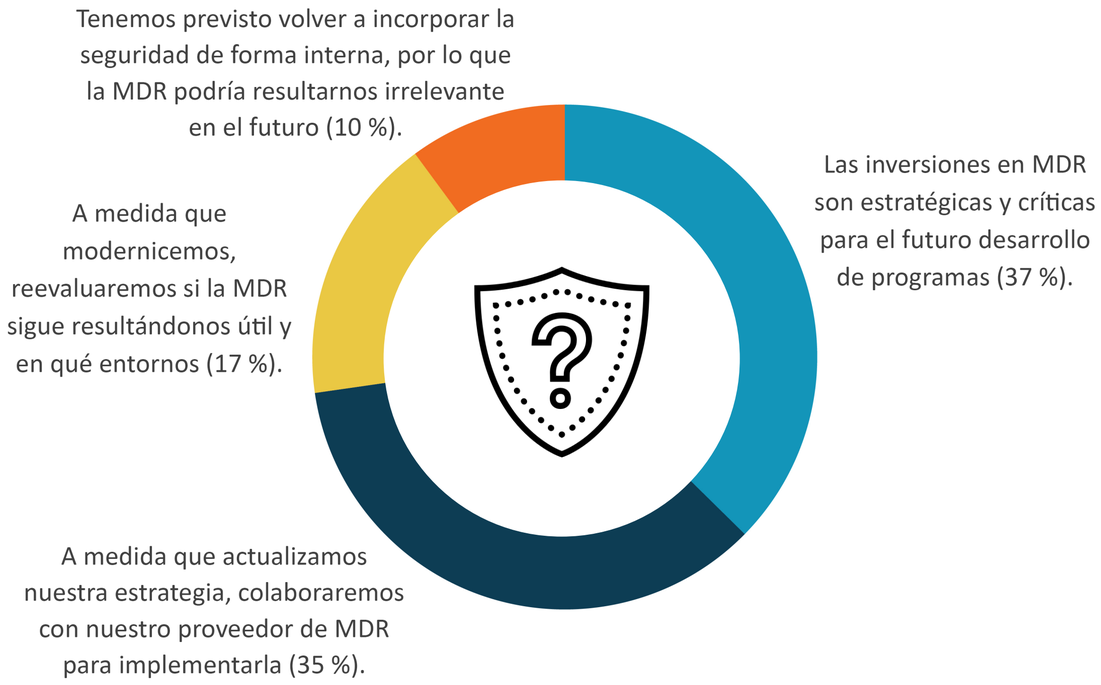
VOLVER AL ÍNDICE

La MDR se está convirtiendo en una estrategia de seguridad estándar

El uso de servicios de MDR se ha convertido en un componente esencial de los programas de estrategia de seguridad, lo que convierte a los proveedores de MDR en socios estratégicos. Ayudan a los equipos de TI y seguridad a acelerar el desarrollo de programas, mejorar el estado de seguridad y obtener otros beneficios menos visibles, como respaldo para los objetivos de cumplimiento normativo, la adquisición de seguros cibernéticos y la mejora de los conocimientos y procesos de seguridad internos. En consecuencia, la mayoría consideran que la MDR es una continuación de sus inversiones en los programas de seguridad. Un 37 % afirman que la MDR es estratégica y crítica, y otro 35 % están planeando colaborar con sus proveedores de MDR para actualizar e implementar futuras estrategias de seguridad.

ESG considera que la MDR representa una estrategia de seguridad importante y estándar, y recomienda a las organizaciones continuar explorando casos de uso adicionales que les permitan acelerar el desarrollo de programas de seguridad y mejorar el estado de seguridad.

Dónde encaja mejor la MDR en el contexto más amplio de la modernización del SOC:



> La mayoría consideran que la MDR es una **continuación de sus inversiones en los programas de seguridad”.**

VOLVER AL ÍNDICE

DELL Technologies

Dell Technologies (en la bolsa de Nueva York: DELL) ayuda a las organizaciones y las personas a crear su futuro digital y transformar su forma de trabajar, vivir y jugar. La empresa proporciona a los clientes la cartera de tecnologías y servicios más amplia e innovadora del sector para la era de los datos.

MÁS INFORMACIÓN

ACERCA DE ESG

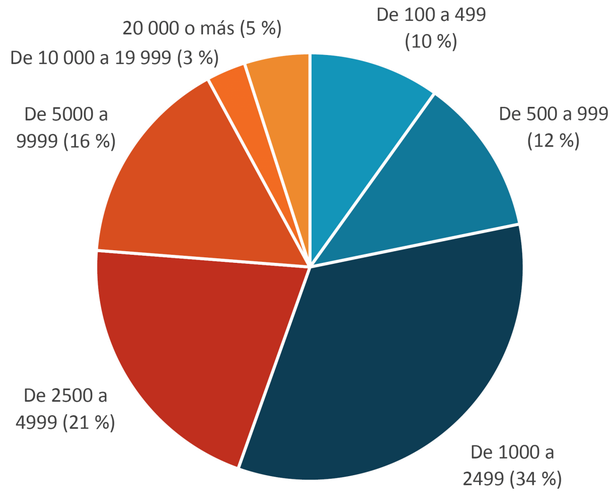
Enterprise Strategy Group es una empresa de análisis de tecnología, investigación y estrategia integrada que proporciona inteligencia de mercado, información procesable y servicios de contenido de comercialización a la comunidad tecnológica internacional.

Metodología de investigación y datos demográficos

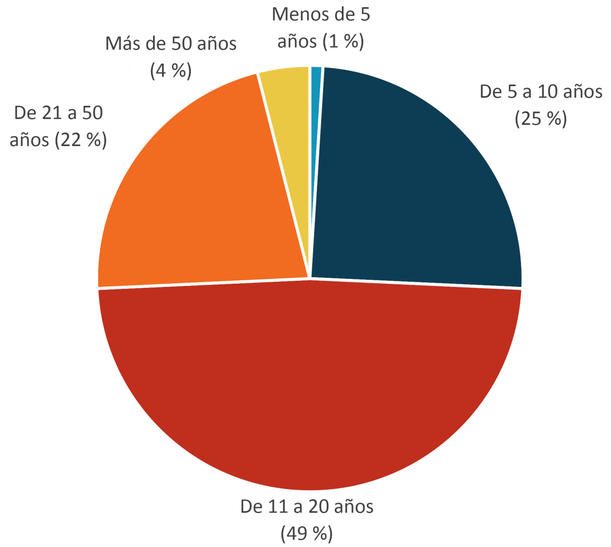
A fin de recopilar datos para este estudio, ESG realizó una exhaustiva encuesta en línea a profesionales de la ciberseguridad de organizaciones del sector privado y público en Norteamérica (Estados Unidos y Canadá), entre el 3 de agosto de 2022 y el 14 de agosto de 2022. Para poder optar a participar, los encuestados debían ser profesionales de la ciberseguridad involucrados personalmente con la tecnología de ciberseguridad, incluyendo productos, servicios y procesos. Todos los encuestados recibieron un incentivo para completar la encuesta en forma de efectivo o equivalentes de efectivo.

Tras filtrar a quienes no cumplían los criterios de inclusión, eliminar las respuestas duplicadas y seleccionar el resto de respuestas completadas (en función de varios criterios) para lograr la integridad de los datos, se utilizó una muestra final total de 373 profesionales de la ciberseguridad.

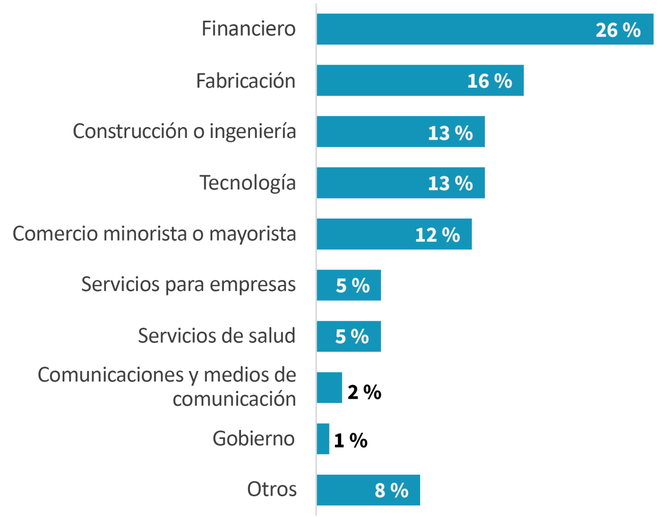
ENCUESTADOS POR NÚMERO DE EMPLEADOS



ENCUESTADOS POR ANTIGÜEDAD DE LA EMPRESA



ENCUESTADOS POR SECTOR



VOLVER AL ÍNDICE

Enterprise Strategy Group es una empresa de análisis de tecnología, investigación y estrategia integrada que proporciona inteligencia de mercado, información procesable y servicios de contenido de comercialización a la comunidad tecnológica internacional.