Eleven Paths

# De MSS a MDR y más allá

¿Qué es lo próximo en Servicios de Ciberseguridad?

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

# 1 | La ciberseguridad hoy

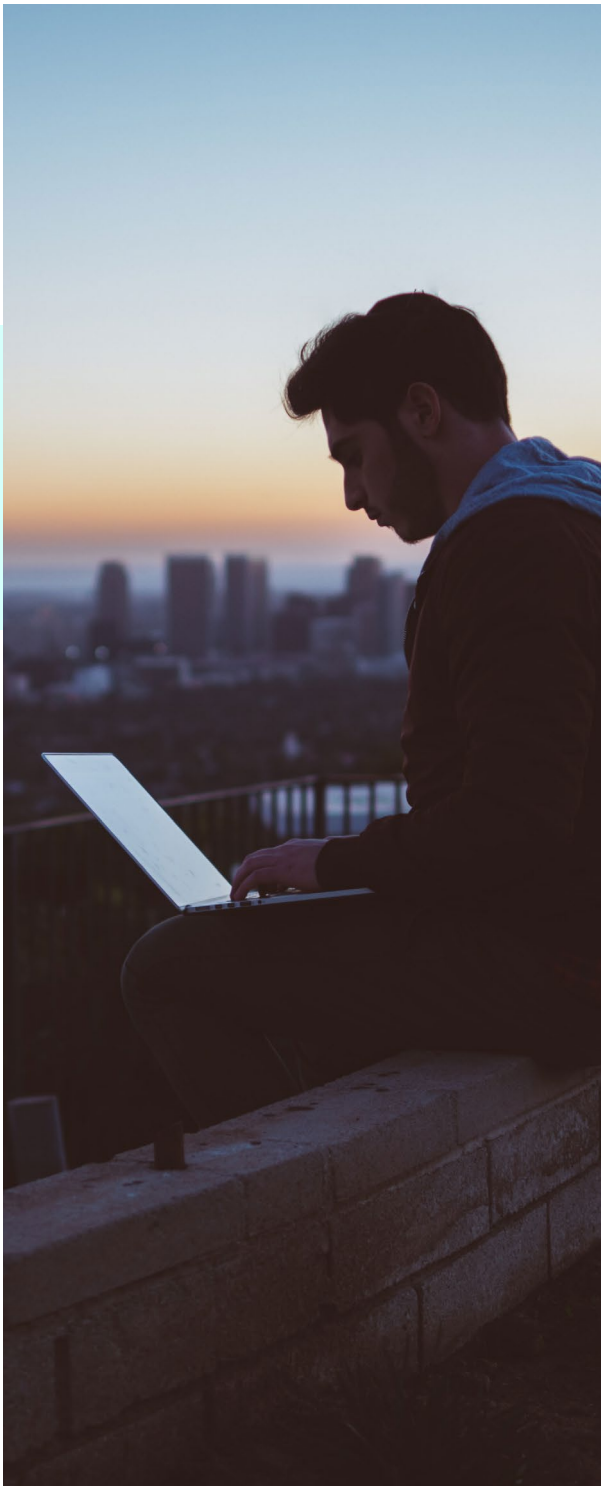
Es nuestra opinión que la ciberseguridad hoy en día está en una encrucijada. A pesar del aumento de la concienciación, el enfoque y la inversión, muchas organizaciones siguen luchando para implementar programas de seguridad eficaces. Por ejemplo, aún después de las secuelas de los primeros ataques globales de *ransomware* en 2017 y las constantes olas posteriores, hemos visto recientemente un aumento de incidentes *ransomeware* graves en nuestra base de clientes y parece que otros proveedores de seguridad están informando de lo mismo:

*En el tercer trimestre de 2020, Check Point Research vio un aumento del 50% en el promedio diario de ataques de rescate, en comparación con la primera mitad del año.*

(https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/)

Está claro que algo no funciona bien en la industria. Se están invirtiendo miles de millones de euros para crear nueva tecnología y destinando parte también hacia los presupuestos de seguridad, pero seguimos siendo muy vulnerables. Desafortunadamente, hay una creciente comprensión y consenso de que nuestras maneras deben cambiar.

Hemos estado buscando una píldora mágica que pueda garantizar la salud, una tecnología o una única acción que pueda prevenir todos los ataques. Como ocurre con muchas enfermedades agudas, la detención de algunos tipos de ataques podría ser atendida completamente con alguna medida específica. Pero garantizar que nuestra organización sea y se mantenga "ciber-saludable" requiere un esfuerzo mucho más minucioso, sistemático y constante.



El NIST ha creado un marco muy completo que explica cómo debe estructurarse dicho programa basado en los pilares de **identificar, proteger, detectar, responder y recuperar.**

**IDENTIFICAR**

- Gestión de Activos
- Gobernanza del Entorno Empresarial
- Evaluación de Riesgos
- Estrategia de Gestión de Riesgos

**PROTEGER**

- Control de Acesso
- Concienciación & Capacitación
- Protección de Datos
- Información sobre Protección & Procedimientos
- Mantenimiento
- Tecnologías de Protección

**DETECTAR**

- Irregularidades & Eventos
- Vigilancia Constante en Seguridad
- Procesos de Detección

**RESPONDER**

- Plan de Respuestas
- Comunicaciones
- Análisis
- Mitigación
- Mejoras

**RECUPERAR**

- Plan de Recuperación
- Mejoras
- Comunicaciones

Sin embargo, su implementación no es una hazaña fácil. Incluso las grandes multinacionales de las industrias reguladas que tienen una larga tradición en la gestión de riesgo y en la creación de capacidades internas de ciberseguridad están luchando con la complejidad y los gastos que ello conlleva.

Los obstáculos son enormes: la **transformación digital** es para muchos un territorio en gran parte inexplorado con riesgos desconocidos; las complejas **cadenas de suministro y las redes de asociados** multiplican las exposiciones; la falta de personal cualificado y los **gastos** disparados hacen que cualquier presupuesto parezca insuficiente; los **cambios de paradigma tecnológico** como el Cloud, el 5G y el IoT hacen que cualquier paso adelante quede rápidamente obsoleto; el **suministro de tecnología de la ciberseguridad** inmanejable y fragmentada es imposible de seguir y evaluar realmente por parte de cualquier organización; los **programas de seguridad** construidos para proteger la red y el IoT están ahora luchando con la complejidad que supone proteger a todo el negocio, la marca y el personal; los **riesgos cibernéticos y físicos** se desdibujan en un continuo. Estamos viendo una mayor necesidad de asesoramiento y de subcontratación para ayudar a que los programas de seguridad evolucionen y se hagan sostenibles y a prueba de futuro.

*Diversas previsiones muestran que el mercado de los servicios de seguridad gestionada crece a tasas de dos dígitos. Un informe de Allied Market Research estima que el mercado alcanzará casi 41.000 millones de dólares para 2022, basándose en una tasa de crecimiento anual compuesta del 16,6% entre 2016 y 2022.*

Si observamos organizaciones más pequeñas, el panorama es aún más preocupante. A medida que el cibercrimen se hace más sofisticado y el gasto de un ataque disminuye, cualquier negocio puede valer la pena. En muchos casos el premio no es ni siquiera la pequeña empresa, sino que puede ser utilizado como un primer paso hacia una mayor captura. Hemos hablado con muchas de estas organizaciones y sus CISO y la realidad en muchos casos es que están empezando de cero después de que un ataque dejara claro que no estaban preparados, y que la dilación ya no era viable. Dichas organizaciones no pueden hacerlo por sí solas realmente, requieren una orientación completa y soluciones integrales. Hemos tenido casos en los que se ha pedido que subcontratáramos, para algunos, la propia función del CISO.

# 2 | De MSS a MDR

Es natural, entonces, que los servicios de seguridad gestionada ya estén en transición de administrar la tecnología y proteger los perímetros a ofrecer servicios completos de detección de amenazas y respuesta.

*"2025, el 50% de las organizaciones utilizarán los servicios de MDR para funciones de vigilancia, detección y respuesta a las amenazas que ofrezcan capacidades de contención."*
*Gartner*

Según Gartner, los servicios de MDR se definen como:

> *Los servicios de gestión, detección y respuesta a las amenazas (MDR) proporcionan a los clientes capacidades de un moderno centro de operaciones de seguridad (SOC) para detectar, analizar, investigar y responder activamente a las amenazas (por ejemplo, contención o interrupción).*
>
> *Los proveedores de servicios MDR ofrecen una experiencia llave en mano, y muchos de ellos utilizan una pila de tecnología predefinida que abarca puntos finales, redes, servicios en nube, tecnología operativa (OT)/Internet de las cosas (IoT) y otras fuentes, para recopilar registros relevantes, datos y otra telemetría (por ejemplo, datos forenses, información contextual).*
>
> *Esta telemetría se analiza a través de la plataforma del proveedor utilizando una gama de análisis, inteligencia de amenazas (TI) y análisis manual de expertos en detección y respuesta a incidentes...*
>
> *Los servicios de caza de amenazas realizados por personas complementan las capacidades de vigilancia y detección en tiempo real para encontrar amenazas nuevas y sofisticadas.*

Este enfoque es definitivamente un gran paso adelante con respecto a los MSS tradicionales que fueron diseñados para centrarse en la seguridad perimetral, la gestión de la tecnología de seguridad, el cumplimiento y el filtrado de alertas, en lugar de en lo que debería ser el resultado real de las operaciones de seguridad: **detección y respuesta.**

También alivia al cliente de tener que soportar la carga de construir toda esta capacidad internamente, algo que en cualquier caso está fuera del alcance de la mayoría de las organizaciones debido a la falta de conocimientos, habilidades, presupuesto o tiempo. Ni siquiera es económicamente viable para las organizaciones más grandes con los bolsillos más llenos, como explicamos antes.

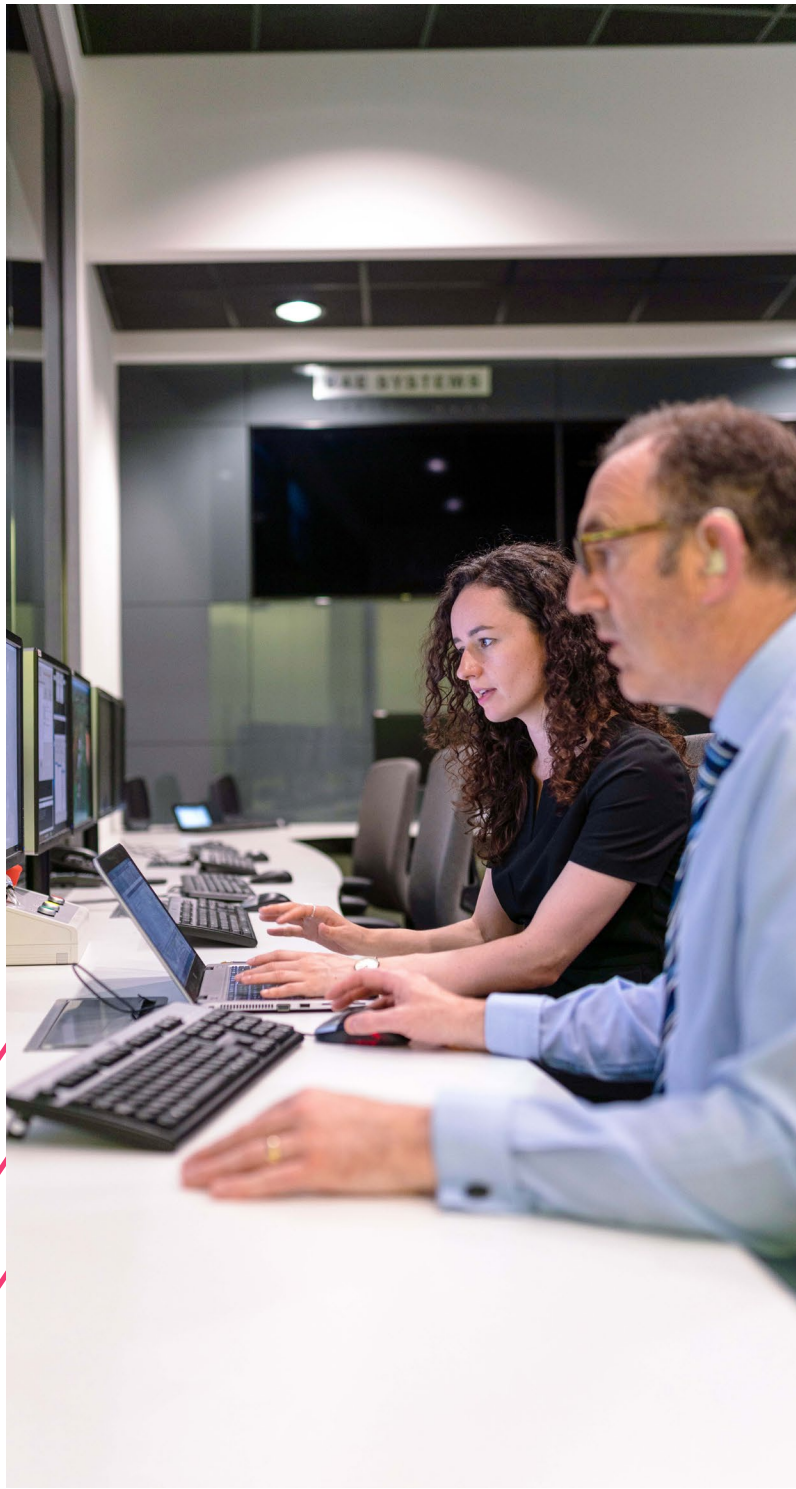
Calculemos algunas **cifras para una gran empresa promedio en Europa** (alrededor de 3.000 empleados):

- **8 operadores SOC de nivel 1** para proporcionar vigilancia 24x7, ya que muchos fallos técnicos o ataques vienen cuando menos conviene.
- Al menos **2 analistas de L2** capaces de realizar una clasificación 8x5, respuesta a incidentes, recopilación de información sobre amenazas, caza, ingeniería de detección aprovechando marcos como MITRE ATT&K para afinar las herramientas.
- Al menos **1 analista L3** capaz de hacer una coordinación avanzada de respuesta a incidentes, investigación, análisis de malware, forense, etc.
- La **tecnología mínima para una visibilidad adecuada** como EDR y SIEM para cubrir 3000 puntos finales.
- Un **equipo para evaluar** entre docenas de productos diferentes y diseñar la solución, además de todas las herramientas rastreadoras de incidentes y tareas automatizadas, la formación y el soporte.

Definitivamente es un programa que a las tarifas actuales del mercado requerirá al menos 900K€ en personal y formación, y más de 300K€ en tecnología, por lo que serían más de 1M€ anuales. **Los servicios de MDR llave en mano** pueden definitivamente proporcionar una barrera de entrada mucho más baja y son la única manera de que las empresas promedio incorporen capacidades efectivas de detección y respuesta en sus programas de seguridad.

Las grandes empresas pueden seguir beneficiándose de los servicios de MDR, aunque de una manera diferente. Es probable que un enfoque "llave en mano" no se integre plenamente con las capacidades existentes que esas organizaciones tienen y desean conservar internamente, y que realmente atiendan a sus necesidades específicas y objetivos comerciales. Necesitan una **oferta de detección y respuesta a las amenazas más personalizada**, que pueda ayudar a llenar las lagunas y reducir los gastos de los aspectos específicos de la MDR y se integre plenamente en su arquitectura de seguridad general y en las operaciones de seguridad ya existentes. Los SLA personalizados y los flujos de trabajo híbridos que permiten el traspaso de tareas entre el proveedor de MDR y el cliente son obligatorios, así como la proximidad geográfica y la estrecha colaboración y comprensión de la seguridad y el negocio de los clientes.

Esto no quiere decir que los servicios de MSS ya no sean necesarios. Sus funciones siguen siendo necesarias, pero deben considerarse como un hecho.
**El protagonismo en cualquier edificio de SOC y el proceso de selección de proveedores debe darse a la detección y respuesta, algo en lo que muchas organizaciones y proveedores aún se quedan cortos.**



# 3 | De MDR y más allá

Todo esto es bueno, pero **¿tener un programa de detección y respuesta eficaz es suficiente para garantizar el éxito de un programa de seguridad?** Desafortunadamente, este no es el caso. Es crucial y obligatorio, pero nuestro programa de seguridad en general fallará si no ponemos la misma atención en todas las otras áreas de operaciones de seguridad y en el programa de seguridad en su conjunto.

Volviendo a nuestro mensaje inicial, no hay una sola píldora mágica. Necesitamos ser capaces de realizar todas las funciones detalladas en marcos como el propuesto por el NIST, e incorporar la ciberseguridad en nuestra operación y gobierno empresarial.

Nuestro programa MDR está condenando una situación en la que los intentos de resolver un problema son poco sistemáticos o superficiales, lo que da lugar sólo a una mejora temporal o menor y el exceso de gastos, no cumplir con los SLA o incluso no evitar completamente la teoría del cisne negro que nuestro negocio tanto teme, a menos que hayamos preparado el terreno adecuadamente en las funciones de identificar y proteger.

El inventario de activos, la evaluación y la gestión de riesgos es donde realmente se sientan las bases. Necesitamos saber **qué proteger, cuáles son las amenazas contra las que debemos protegerlos y cuál es nuestra exposición a ellas.**

*En una encuesta realizada a casi 3.000 profesionales de la seguridad informática, el Ponemon Institute descubrió que, a pesar de dedicar más recursos a la gestión de las vulnerabilidades, las organizaciones todavía no son capaces de minimizar los riesgos de un ataque. Sólo la mitad de los encuestados dijeron que podían detectar rápidamente las vulnerabilidades y responder a los ataques, y sólo el 44% dijo que podían aplicar parches rápidamente.*

En las tareas menos atractivas como el seguimiento de los activos, la aplicación de parches a los sistemas y la gestión de las vulnerabilidades es donde muchas veces se pierde la batalla, antes de tener la oportunidad de detectar y responder.

En realidad, muy pocos ataques se basan en los 0-days. La mayoría de los ataques aprovechan vulnerabilidades conocidas que se cuelan por las grietas. Es una tarea difícil para cualquier organización rastrear todos los activos, encontrar sus exposiciones, detectar todas las vulnerabilidades y corregirlas a tiempo. La priorización de las vulnerabilidades según la probabilidad y el riesgo es todavía un problema abierto para los programas de gestión de vulnerabilidades. Y para empeorar las cosas, no todas las vulnerabilidades pueden ser encontradas por los escáneres automáticos. A veces existen algunas más sutiles en aplicaciones específicas o en sistemas enteros que sólo pueden encontrar los *pentest* o los sombreros blancos.

La **capacidad de la inteligencia de amenazas para comprender mejor a nuestros adversarios también es crucial** en el proceso de gestión de riesgos y debería impulsar la capa de protección necesaria para hacer viable la detección y la respuesta. También puede ayudar a alertarnos sobre nuevas amenazas específicas que están surgiendo e incluso puede ser la única forma de defender nuestros activos digitales como nuestra marca, nuestra reputación o la propiedad intelectual contra los ataques en el espacio digital. Incluso cuando se responde a un incidente, disponer de información sobre el ataque, el actor o la campaña puede simplificar enormemente el proceso de respuesta al permitir una adecuada priorización y probar la información y orientación del contexto. No obstante, muy pocas organizaciones disponen de capacidades de inteligencia de amenazas para prepararse, detectar y responder mejor.

La protección, aunque nunca puede ser perfecta, tiene que ayudar a reducir el riesgo y reducir el número de eventos de seguridad a un nivel manejable para que la función de detección y respuesta tenga alguna posibilidad de completar su misión. Y con la llegada del Cloud, el IoT, el cambio de los trabajadores de la oficina a casa (teletrabajo) usando dispositivos y redes desconocidas, este es un desafío abierto.

Creemos que la mayoría de las organizaciones se beneficiarán definitivamente de un socio MDR, pero probablemente lo hará más desde un **socio "todo en uno" que puede al mismo tiempo ayudarles a construir un programa de ciberdefensa más completo**. Un socio que pueda ofrecer esto como una solución integrada, que pueda adaptarse a sus necesidades particulares, que esté cerca de ellos y entienda su negocio. Un socio que entienda la tecnología, que tenga conocimiento del panorama de las amenazas y que sepa por experiencia lo que implica proteger un negocio digital, un socio que pueda innovar y ayudarles a estar preparados para todo lo que está cambiando en el mundo hoy en día.

Creemos que se requiere unos servicios gestionados a otro nivel, y estamos preparados para ofrecer exactamente esto.

No le quite el ojo a ElevenPaths para lo que trae en la ciberdefensa...

# Sobre ElevenPaths

ElevenPaths es la compañía de ciberseguridad de Telefónica, integrada dentro del holding Telefónica Tech, que aglutina los negocios digitales con mayor potencial de crecimiento de la compañía.

En un mundo en el que las ciberamenazas son inevitables, como proveedores de servicios de seguridad gestionada inteligente, nos enfocamos en prevenir, detectar, dar respuesta y disminuir los posibles ataques a los que se enfrentan las empresas. Garantizamos la ciber-resiliencia de nuestros clientes a través de un soporte 24/7 gestionado desde once i-SOC alrededor del mundo con capacidad operativa global.

Creemos en la idea de desafiar el estado actual de la seguridad, c aracterística que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y, de esta manera, logramos ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Trabajamos para garantizar un entorno digital más seguro a través de alianzas estratégicas que nos permitan mejorar la seguridad de nuestros clientes, así como a través de colaboraciones con organismos y entidades líderes como la Comisión Europea, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, EuroPol, Incibe, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Centro de Ciberseguridad Industrial (CCI) y APWG.

**Más información**

**elevenpaths.com** | **@ElevenPaths** | **blog.elevenpaths**