ESPECIAL

CIBERRESILIENCIA EN LA ERA DE LA IA

Ciberresiliencia en la era de la IA: adaptarse ya no es una opción

IR A PÁGINA SIGUIENTE

Ciberresiliencia en la era de la IA: adaptarse ya no es una opción

La ciberresiliencia deja de medirse por la capacidad para recuperarse de un incidente y pasa a definirse por la rapidez con la que una organización es capaz de adaptarse a un entorno que cambia constantemente.

Rosalía Arroyo

Durante años, hablar de ciberresiliencia era hablar de recuperación. El objetivo consistía en preparar a las organizaciones para resistir un ciberataque, minimizar su impacto y volver a la normalidad en el menor tiempo posible. Los planes de continuidad de negocio, las copias de seguridad o los procedimientos de respuesta ante incidentes se convirtieron en los pilares sobre los que se construía esa capacidad de recuperación. Todo eso sigue siendo importante. Lo que ha cambiado es el escenario en el que esa respuesta tiene que producirse.

Las empresas ya no operan en entornos relativamente estables, sino en escenarios mucho más dinámicos en el que los responsables de seguridad ya no solo tienen que proteger unos activos concretos, sino gestionar un entorno que cambia prácticamente a diario.

Por eso, la conversación sobre ciberresiliencia también está cambiando. Recuperarse después de un ataque sigue siendo imprescindible, pero ya no basta. Hoy la resiliencia empieza mucho antes del incidente y continúa mucho después.

Es más, en realidad, el mayor reto ya no consiste únicamente en hacer frente a un atacante, consiste en mantener el control mientras todo lo demás cambia.

Cuando el problema deja de ser la falta de información

Hace apenas una década, uno de los principales desafíos de los equipos de seguridad era la falta de visibilidad. Existían puntos ciegos, las capacidades de detección eran limitadas y obtener información útil sobre lo que estaba ocurriendo en la infraestructura resultaba complicado.

La situación actual es casi la contraria.

Las organizaciones generan hoy una cantidad de información sin precedentes. Firewalls, plataformas EDR y XDR, herramientas de identidad, aplicaciones cloud, dispositivos conectados, servicios SaaS o sistemas industriales producen millones de eventos cada día. A ellos se suman fuentes de inteligencia de amenazas, análisis automatizados y capacidades de inteligencia artificial capaces de identificar comportamientos anómalos en cuestión de segundos.

Paradójicamente, disponer de más información no siempre facilita la toma de decisiones.

> La ciberresiliencia no se mide únicamente por la capacidad para recuperarse de un incidente, sino por la rapidez con la que una organización es capaz de adaptarse al cambio

Muchos responsables de seguridad reconocen que el verdadero desafío ya no consiste en descubrir amenazas, sino en determinar cuáles requieren realmente atención. Las alertas aumentan, las herramientas se especializan y los datos crecen a un ritmo muy superior a la capacidad de los equipos para analizarlos. En ese contexto, la ciberresiliencia depende tanto de la capacidad para detectar un incidente como de la capacidad para interpretar correctamente el contexto y priorizar aquello que realmente puede poner en riesgo el negocio.

La inteligencia artificial está contribuyendo a aliviar parte de esa presión, pero también añade una nueva capa de complejidad. Los modelos deben gobernarse, los datos utilizados necesitan protección y las propias herramientas de IA pasan a formar parte de la superficie de exposición de las organizaciones.

Por primera vez, la tecnología que ayuda a reducir la complejidad también contribuye a crear nuevos desafíos de seguridad.

La inteligencia artificial acelera un cambio que ya estaba en marcha

Es fácil pensar que la inteligencia artificial ha transformado por completo la ciberseguridad. En realidad, lo que ha hecho ha sido acelerar una evolución que ya estaba en marcha. La migración al cloud, la digitalización de procesos, el trabajo híbrido, la automatización o la proliferación de aplicaciones conectadas ya estaban obligando a las organizaciones a replantear su estrategia de seguridad. La IA ha multiplicado la velocidad de ese cambio.

Su impacto va mucho más allá de la aparición de nuevos ataques generados automáticamen-

te o de campañas de phishing más convincentes. Cada vez más organizaciones incorporan asistentes inteligentes, modelos generativos y agentes capaces de ejecutar tareas de forma autónoma, que acceden a aplicaciones corporativas, consultan bases de datos, generan documentos o interactúan con otros servicios.

Eso obliga a replantear muchas de las preguntas que hasta hace poco parecían resueltas. Ya no basta con verificar la identidad de un usuario o controlar el acceso a una aplicación. También es necesario decidir qué puede hacer un agente de IA, con qué información puede trabajar, qué acciones puede ejecutar y cómo garantizar la trazabilidad de todas esas operaciones.

La propia noción de identidad empieza a cambiar. Muchas organizaciones gestionan ya más identidades no humanas que usuarios tradicionales, lo que obliga a revisar los modelos de autenticación, autorización y gobierno del acceso.

La resiliencia deja así de ser un estado al que se llega para convertirse en un proceso continuo de adaptación.

La complejidad se ha convertido en el principal enemigo

Si hubiera que resumir en una sola palabra el reto al que se enfrentan hoy los responsables de seguridad, probablemente sería complejidad.

Nunca habían dispuesto de tantas tecnologías para proteger sus organizaciones. Nunca habían tenido tanta capacidad para detectar comportamientos anómalos, recopilar inteligencia o automatizar tareas. Sin embargo, tampoco habían tenido que gestionar un ecosistema tan amplio y diverso.

El riesgo no siempre surge por la ausencia de protección: una configuración incorrecta, un permiso excesivo, una credencial olvidada o una aplicación desplegada sin el conocimiento del equipo de seguridad pueden convertirse en la puerta de entrada para un ataque.

El mayor desafío para los equipos de seguridad ya no es recopilar más datos, sino convertirlos en decisiones útiles y oportunas

No es casualidad que conceptos como plataforma, automatización, inteligencia contextual o detección y respuesta gestionadas estén ganando protagonismo. Todos responden a una misma necesidad: reducir la complejidad para mejorar la capacidad de adaptación.

Y, probablemente, esa sea una de las principales diferencias entre la ciberresiliencia de ayer y la de hoy. Antes el objetivo era resistir un ataque. Ahora también consiste en ser capaz de seguir evolucionando sin que esa evolución se convierta en una nueva fuente de riesgo.

La resiliencia como ventaja competitiva

Durante mucho tiempo, la ciberseguridad se entendió como una función destinada a reducir

Antes bastaba con recuperarse. Hoy hay que adaptarse.

Hace unos años	Hoy
El objetivo era recuperarse tras un incidente.	**El objetivo es adaptarse continuamente a un entorno cambiante.**
La prioridad era proteger el perímetro.	**La prioridad es proteger identidades, datos, aplicaciones y servicios, estén donde estén.**
Los usuarios eran el principal foco de atención.	**Personas, aplicaciones, máquinas y agentes de IA forman parte del nuevo ecosistema de identidades.**
Más herramientas significaban más protección.	**La resiliencia se mide por la capacidad de anticiparse, responder y evolucionar sin perder el control.**
La seguridad se medía por la capacidad de resistir un ataque.	**Reducir la complejidad y ganar contexto es tan importante como incorporar nuevas capacidades.**

riesgos. Hoy, prácticamente cualquier iniciativa de transformación digital lleva asociada una decisión sobre ciberseguridad, por lo que la seguridad deja de ser un elemento que acompaña al negocio para convertirse en un factor que condiciona su capacidad para evolucionar.

Por eso, la ciberresiliencia ya no puede entenderse únicamente como una disciplina orientada a responder ante incidentes. También representa la capacidad de una organización para incorporar nuevas tecnologías, adaptarse a cambios regulatorios, integrar modelos de trabajo diferentes o aprovechar la innovación sin perder el control sobre sus activos más críticos. Esa transformación también está modificando el papel de los responsables de seguridad. Además de proteger la organización, se espera de ellos que ayuden a tomar decisiones, aporten contexto sobre los riesgos y faciliten que la innovación pueda desarrollarse de forma segura. En otras palabras, la resiliencia deja de medirse únicamente por la capacidad para recuperarse de un ataque y empieza a hacerlo por la capacidad para seguir avanzando incluso en un entorno de incertidumbre.

La inteligencia artificial marcará buena parte de esa evolución durante los próximos años, pero no será el único desafío. La expansión de las identidades no humanas, la protección del dato, la adaptación a nuevas regulaciones, la gestión de la criptografía o la creciente dependencia de terceros seguirán obligando a revisar continuamente las estrategias de seguridad.

Quizá esa sea la mayor diferencia respecto a hace apenas unos años. Antes, la ciberresiliencia se preparaba para responder a un incidente. Hoy se construye cada día, acompañando la evolución del negocio, anticipando riesgos y adaptándose de forma continua a un entorno en el que el cambio ha dejado de ser una excepción para convertirse en la nueva normalidad. CST

La ciberresiliencia vista por quienes la gestionan cada día

La ciberresiliencia ya no se construye únicamente con más tecnología. También exige simplificar la complejidad, gobernar el uso de la inteligencia artificial, reforzar la colaboración con el negocio y prepararse para responder a amenazas que evolucionan constantemente. Seis responsables de tecnología y ciberseguridad de Servatrix, Top Doctors, FUNDAE, Mutualia, MasOrange y Siemens analizan cómo está cambiando su forma de proteger las organizaciones y cuáles serán las prioridades que marcarán la resiliencia en los próximos años.

Rosalía Arroyo

Si hace apenas unos años la conversación giraba alrededor del perímetro, hoy los responsables de seguridad hablan de identidades, datos, resiliencia y capacidad de adaptación. La expansión de la nube, el trabajo híbrido y, más recientemente, la inteligencia artificial han obligado a replantear estrategias que hasta hace poco parecían consolidadas.

Uno de los cambios más evidentes ha sido el abandono del modelo tradicional de seguridad perimetral. Las organizaciones ya no operan desde una única red corporativa y la infraestructura se ha distribuido entre múltiples nubes, aplicaciones y servicios. En este contexto, proteger el acceso a la información resulta más importante que proteger un perímetro físico.

Alejandro Expósito Esteban, Digital, Innovation and Business Operations Director de Servatrix, resume esta evolución al señalar que “la seguridad ya no se juega en el perímetro, sino en la identidad, los datos y el contexto”. Cree que el reto pasa por validar quién accede, desde dónde y con qué propósito, limitando los privilegios al mínimo necesario para proteger unos activos cuyo valor reside, sobre todo, en el conocimiento.

En el ámbito sanitario, Bernardo Ruiz, Chief Technical Officer de Top Doctors, sostiene que “ya no existe un ‘dentro’ de la oficina que proteger”. La seguridad, explica, se ha integrado en la propia arquitectura tecnológica y obliga a verificar de forma continua identidades, dispositivos y transacciones.

A esa transformación se suma otro factor: la creciente complejidad de los entornos tecnológicos. David Reinares, Cybersecurity BP CYS / GBS / P&O de Siemens, apunta que la consolidación de arquitecturas híbridas y multicloud, el trabajo remoto y la creciente dependencia de terceros han obligado a reforzar la protección de identidades, la seguridad en la nube y la gestión del riesgo asociado a proveedores y a la cadena de suministro de software. En su opinión, este escenario exige avanzar hacia mo-

La ciberresiliencia ya no consiste únicamente en recuperarse de un ataque, sino en adaptarse de forma continua al cambio

delos de seguridad por diseño y arquitecturas Zero Trust cada vez más maduras.

Pero el cambio no ha sido solo tecnológico. Para muchos responsables de seguridad, el verdadero punto de inflexión ha consistido en asumir que la ciberseguridad ya no puede recaer exclusivamente en el departamento de Sistemas. Iratxe Ijalba Izagirre, Directora de Sistemas de Informaciónde Mutualia, explica que se ha evolucionado desde un enfoque centrado en la protección hacia otro que combina prevención, detección, respuesta y recuperación. La continuidad de negocio, la revisión de accesos, la gestión de proveedores o los simulacros forman hoy parte de una estrategia mucho más amplia.

La dimensión cultural también resulta determinante para Andrés García, Project Manager e IT Projects Coordinator de Masorange. Explica que, durante los últimos años en MasOrange se han reforzado los equipos especializados, la inversión en herramientas y los programas de formación, pero considera que el avance más importante ha sido entender que la seguridad es una responsabilidad compartida por toda la organización y no únicamente por un área especializada.

La inteligencia artificial añade una nueva capa de transformación. Carlos Juarros Huerga, CISO de Fundae (Fundación Estatal para la Formación en el Empleo), la define como el cambio más disruptivo de los últimos años, tanto por las oportunidades que abre como por los riesgos que introduce. A su juicio, cualquier proyecto basado en IA debe evaluarse también desde la perspectiva de la seguridad, la protección de datos, el cumplimiento normativo y la continuidad del negocio. “La ciberseguridad ha dejado de ser una capa defensiva para convertirse en una condición necesaria para que la organización pueda innovar y seguir funcionando con confianza”, afirma.

“La seguridad ya no se juega en el perímetro, sino en la identidad, los datos y el contexto”

Alejandro Expósito Esteban, Digital, Innovation and Business Operations Director, **Servatrix**

La complejidad, el gran enemigo de la ciberresiliencia

La tecnología ya no es el principal problema. Gestionarla sí. Aunque cada organización

afronta desafíos diferentes, la mayoría de los responsables consultados coincide en que el verdadero obstáculo para mejorar la ciberresiliencia no es la falta de herramientas, sino la dificultad para administrar entornos cada vez más distribuidos, con múltiples proveedores, aplicaciones, identidades y servicios conectados.

"El principal obstáculo no es la falta de tecnología; es la complejidad operativa", asegura Alejandro Expósito, explicando que las organizaciones acumulan capas de infraestructura —cloud, SaaS, sistemas internos, laboratorios o terceros— y que "mantener controles consistentes en todo eso es difícil". Por eso, defiende que la resiliencia sólo mejora cuando la seguridad "se gestiona como una capacidad operativa continua, no como un proyecto que se termina".

La misma idea aparece en la reflexión de David Reinares, para quien el gran desafío pasa por "la gestión efectiva de la complejidad y la visibilidad en entornos distribuidos y dinámicos". La fragmentación de las soluciones de seguridad, la dificultad para conocer en todo momento qué activos existen, quién accede a ellos o cómo están configurados, junto con "la sobre-

"Ya no existe un 'dentro' de la oficina que proteger: la seguridad debe verificar continuamente identidades, dispositivos y transacciones"

Bernardo Ruiz,
Chief Technical Officer, **Top Doctors**

carga de alertas y ruido", dificultan que incluso los equipos más preparados puedan identificar qué amenazas requieren realmente atención. Para responder a esta realidad, apuesta por consolidar plataformas, automatizar procesos y apoyarse en la inteligencia artificial para ganar eficiencia.

Pero la complejidad no es únicamente tecnológica. Carlos Juarros sitúa el foco en la gobernanza. "El principal obstáculo no es únicamente tecnológico. Es de gobernanza, priorización y coordinación", afirma. A su juicio, muchas organizaciones cuentan con herramientas y controles suficientes, pero "no siempre tienen una visión suficientemente integrada del riesgo, de las dependencias críticas o de los impactos reales de una interrupción". De ahí que defienda mecanismos claros de gobierno y una toma de decisiones basada en el riesgo.

La cultura de la organización es otra pieza fundamental. Iratxe Ijalba considera que "el principal obstáculo es conseguir que la ciberseguridad forme parte del día a día sin que se viva como una carga". Recuerda que disponer de buenas herramientas sirve de poco si las personas no entienden el sentido de los controles o no saben cómo reaccionar ante un incidente. Además, advierte de que la creciente interdependencia entre aplicaciones, proveedores y áreas de negocio obliga a preparar la respuesta

> "El principal reto no es únicamente tecnológico; es de gobernanza, priorización y coordinación"
>
> **Carlos Juarros Huerga,**
> CISO, **FUNDAE**

desde una perspectiva mucho más transversal. No todos los participantes, sin embargo, señalan el mismo problema. Para Andrés García, el mayor freno sigue siendo "la escasez de talento especializado". Aunque las empresas inviertan cada vez más en herramientas y capacidades, reconoce que resulta difícil captar y retener profesionales capaces de operarlas y anticiparse a las amenazas. "Los procesos los ejecutan personas", recuerda, por lo que la pérdida continua de talento termina afectando directamente a la capacidad de respuesta.

Bernardo Ruiz lleva el debate un paso más allá y plantea una reflexión de fondo. "La ciberresiliencia no consiste en evitar que te ataquen; eso es imposible", afirma. El verdadero reto, sostiene, consiste en desarrollar "la capacidad de absorber el impacto y seguir operando sin que el servicio se caiga". Para lograrlo, considera imprescindible dejar de entender la ciberseguridad como un simple requisito normativo o un coste e integrarla plenamente en la estrategia del negocio.

La IA obliga a defenderse en dos frentes

Ninguna tecnología ha cambiado tan deprisa el equilibrio entre atacantes y defensores como la inteligencia artificial. Los responsables consultados coinciden en que el principal riesgo ya no es únicamente disponer de ciberdelincuentes con herramientas más potentes, sino enfrentarse a ataques mucho más rápidos, personalizados y difíciles de detectar. Al mismo tiempo, las propias organizaciones deben aprender a incorporar la IA sin generar nuevas vulnerabilidades.

Alejandro Expósito resume bien esa aceleración: "La IA acorta el tiempo entre el primer error y el impacto". El auge de campañas de phishing altamente dirigidas, el vishing o los deepfakes incrementa el riesgo de compromiso de identidades, una de las principales puertas de entrada para los atacantes. En organizaciones dedicadas a la investigación, además, el problema va más allá del acceso a los sistemas. "Una filtración no es un incidente más: puede cambiar la ventaja competitiva", advierte, al referirse a la protección de la propiedad intelectual y del conocimiento científico.

En el ámbito sanitario, Bernardo Ruiz comparte esa inquietud. A su juicio, lo más preocupante es "la automatización e hiperpersonalización del fraude a gran escala". Los modelos de lenguaje ya permiten crear campañas de ingeniería social prácticamente indistinguibles de una comunicación legítima y, al mismo tiempo, la incorporación de agentes inteligentes abre nuevas

“Necesitamos proveedores que actúen como socios de verdad, capaces de entender nuestro contexto y ayudarnos a priorizar”

Iratxe Ijalba Izagirre,
Directora de Sistemas de Información, **Mutualia**

superficies de ataque, desde el envenenamiento de datos hasta la manipulación de prompts. En este contexto, la resiliencia pasa también por proteger la integridad y la privacidad de la información que alimenta esos modelos.

Pero la amenaza no procede únicamente del exterior. Carlos Juarros distingue claramente dos planos. Por un lado, el uso ofensivo de la IA por parte de los atacantes, capaz de acelerar y escalar técnicas que ya existían. Por otro, “el uso interno no gobernado de herramientas de IA”. Incorporar estas soluciones sin inventario, sin análisis de riesgos o sin controles sobre los datos, advierte, puede abrir nuevas vías de fuga de información o generar dependencias difíciles de gestionar. Por eso insiste en que la IA debe desplegarse con un marco sólido de gobierno, trazabilidad y seguridad desde el diseño.

Ese equilibrio entre innovación y control también preocupa a Andrés García. Aunque reconoce que el uso ofensivo de la IA está haciendo los ataques “más sofisticados, rápidos y difíciles de detectar”, cree que uno de los grandes desafíos consiste en gestionar el riesgo derivado del uso interno de estas herramientas sin

frenar el potencial de innovación que ofrecen a las organizaciones.

La evolución de la ingeniería social ocupa igualmente un lugar destacado en la reflexión de Iratxe Ijalba. En su opinión, la IA está haciendo que los ataques resulten mucho más creíbles, hasta el punto de que "ya no podemos confiar sólo en la intuición o en detectar errores evidentes". Correos perfectamente redactados, mensajes adaptados al contexto o suplantaciones mediante voz e imagen obligan a reforzar los hábitos de verificación y a confirmar por otros canales aquellas solicitudes con impacto económico o acceso a información sensible. Al mismo tiempo, recuerda que la IA también puede convertirse en una aliada para analizar patrones, priorizar alertas o detectar comportamientos anómalos, siempre que su uso esté correctamente gobernado.

David Reinares amplía esa visión al señalar que el verdadero desafío reside en "la velocidad y la escala con la que la IA generativa puede ser utilizada para amplificar y personalizar ataques de ingeniería social y desinformación". Los deepfakes, la automatización en la creación de malware o las campañas masivas de desinformación erosionan la confianza digital y reducen el tiempo disponible para responder. Frente a ello, explica que Siemens está reforzando el gobierno de la IA, desarrollando soluciones propias e incorporando inteligencia artificial para automatizar la detección de anomalías, la gestión de vulnerabilidades y la respuesta ante incidentes.

> "El mayor desafío sigue siendo encontrar y retener el talento necesario para responder a amenazas cada vez más sofisticadas"
>
> **Andrés García,** Project Manager e IT Projects Coordinator, **Masorange**

De proveedores a socios de la resiliencia

La ciberresiliencia tampoco se construye en solitario. A medida que las infraestructuras se vuelven más complejas y aumenta la dependencia de servicios externos, los responsables de seguridad esperan mucho más de fabricantes y proveedores tecnológicos. Ya no basta con ofrecer una buena solución: demandan productos seguros desde el diseño, integración entre plataformas, transparencia y un compromiso real durante todo el ciclo de vida de la tecnología.

Alejandro Expósito resume esas expectativas en tres grandes prioridades: seguridad por defecto y verificable, integración y reducción de ruido y enfoque en resiliencia real. A ello añade una exigencia cada vez más relevante: disponer de garantías técnicas y contractuales sobre cómo se protegen los datos y el conocimiento cuando se utilizan plataformas y modelos de inteligencia artificial.

La necesidad de simplificar la operación también está muy presente en la visión de David Reinares. Reclama "un compromiso inquebrantable con la integración, la automatización inteligente y la transparencia" para reducir la complejidad que hoy soportan los equipos de seguridad. En su opinión, fabricantes y proveedores deben facilitar la interoperabilidad entre plataformas, automatizar las tareas repetitivas, comunicar con rapidez cualquier vulnerabilidad y colaborar estrechamente con sus clientes cuando se produce una crisis. También considera imprescindible avanzar hacia un desarrollo responsable de soluciones de inteligencia artificial aplicadas a la ciberseguridad.

La transparencia aparece como otra de las grandes demandas. Carlos Juarros sostiene que los proveedores deben asumir la seguridad como una parte inseparable del producto y no como una funcionalidad añadida. "A los proveedores ya no podemos pedirles sólo funcionalidad; debemos exigirles seguridad, transparencia, cumplimiento y resiliencia por defecto", afirma. En el caso de las soluciones basadas en IA, reclama

"La gestión de la complejidad y la visibilidad en entornos distribuidos será decisiva para mejorar la ciberresiliencia"

David Reinares,
Cybersecurity BP CYS / GBS / P&O, **Siemenss**

garantías sobre la protección de los datos, la trazabilidad, el control de accesos y el cumplimiento de la normativa.

Más allá de la tecnología, Iratxe Ijalba reivindica una relación mucho más cercana con los proveedores. Las organizaciones, asegura, necesitan "socios de verdad", capaces de entender su contexto, ayudarles a priorizar riesgos y ofrecer información clara cuando aparece una vulnerabilidad crítica o se produce un incidente. "El tiempo y la claridad son clave", recuerda. Al fin y al cabo, añade, "nuestra resiliencia también depende de la resiliencia de quienes forman parte de nuestro ecosistema tecnológico".

Bernardo Ruiz comparte esa visión colaborativa, aunque pone el acento en la seguridad por diseño y en la integración nativa entre soluciones. En lugar de incorporar nuevas herramientas aisladas que incrementen el ruido y los falsos positivos, defiende que los fabricantes actúen como un escudo proactivo dentro de la cadena de suministro de software y faciliten tanto la operación diaria como el cumplimiento normativo.

Para Andrés García, todas esas expectativas pueden resumirse en una palabra: confianza. Confianza en que los socios tecnológicos sean capaces de evolucionar al mismo ritmo que las amenazas, anticiparse a las nuevas técnicas empleadas por los atacantes y ofrecer mecanismos de protección igual de avanzados.

ESET: “La inteligencia de amenazas será un recurso clave para la ciberresiliencia”

Aunque la inteligencia artificial ha acelerado la evolución del panorama de amenazas, para Josep Albors, responsable de Investigación y Concienciación de ESET, los principios de la ciberresiliencia siguen siendo los mismos: “Una empresa ciberresiliente es esa empresa que sabe a lo que se enfrenta”.

Rosalía Arroyo

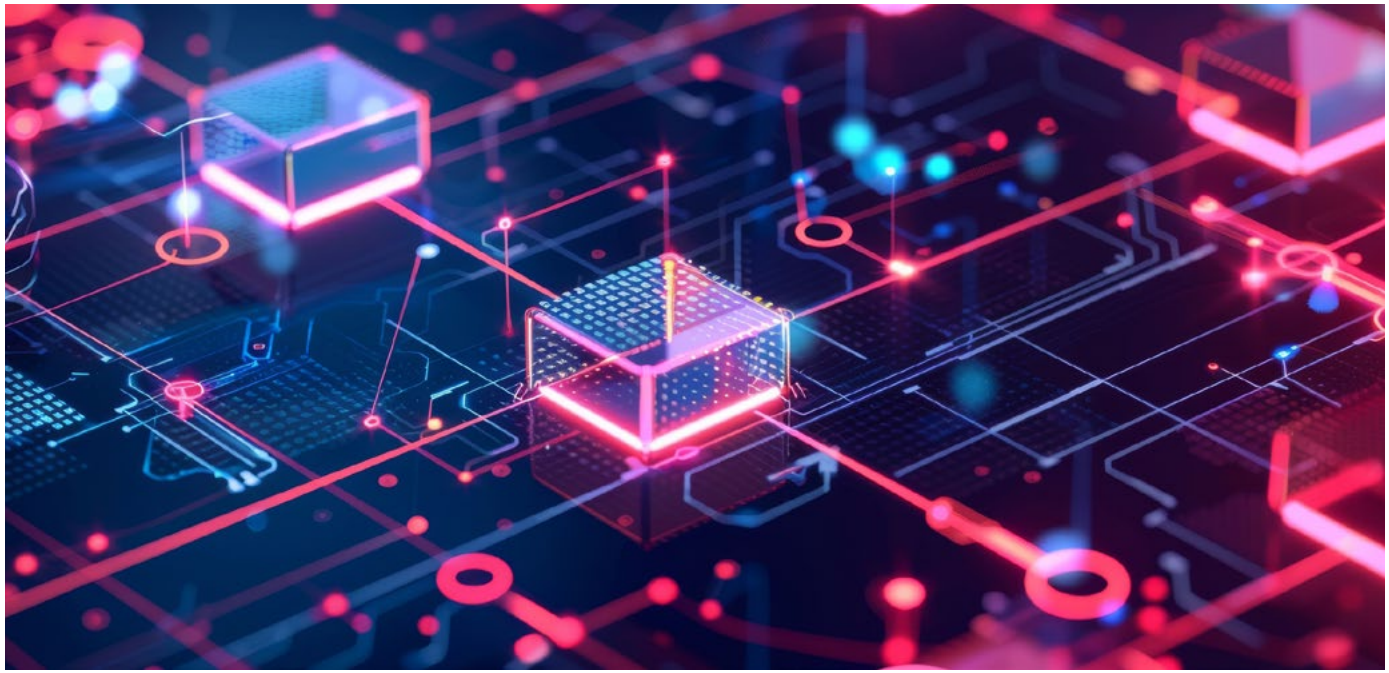
Josep Albors, responsable de Investigación y Concienciación de **ESET,**

A partir de ese conocimiento las organizaciones deben construir una estrategia sólida que les permita adaptarse a la evolución de los ciberdelincuentes sin olvidar los fundamentos de la seguridad, explica, añadiendo que “sin unas bases bien asentadas, por mucha tecnología o muchas herramientas que incorporemos, no va a ser efectivo”.

La IA amplifica las amenazas, pero no cambia sus fundamentos

En su opinión, uno de los errores más habituales consiste en atribuir a la inteligencia artificial cambios que, en realidad, ya venían produciéndose desde hace años. La IA ha incrementado el volumen de amenazas y ha facilitado que actores con menos conocimientos técnicos puedan lanzar campañas más sofisticadas, pero la mayoría de los ataques siguen apoyándose en técnicas bien conocidas. Sí han aparecido nuevos vectores relacionados con la propia adopción de la IA por parte de las organizaciones, especialmente cuando se despliegan agentes, modelos o herramientas sin tener en cuenta los riesgos de seguridad. “Se están implementando herramientas sin tener en cuenta el impacto que pueden tener en la seguridad y eso lo están aprovechando los atacantes”, explica. Para Albors, el problema no reside en la tecnología, sino en la rapidez con la que se está incorporando a los procesos de negocio sin evaluar adecuadamente sus implicaciones desde el punto de vista de la ciberseguridad.

> “No se pueden implementar herramientas de IA sin tener en cuenta la seguridad”



Al mismo tiempo, la inteligencia artificial también está ayudando a reforzar las capacidades defensivas. Albors recuerda que el sector lleva años utilizando algoritmos de aprendizaje automático, modelos de IA y otras técnicas avanzadas para gestionar el enorme volumen de alertas que generan las plataformas de seguridad. En el caso de ESET, los laboratorios analizan alrededor de 700.000 amenazas al día, una cifra que sería imposible gestionar únicamente mediante intervención humana. El objetivo de estas tecnologías no es sustituir a los analistas, sino automatizar las tareas repetitivas y permitir que los equipos se concentren en aquellos incidentes que realmente pueden comprometer a una organización. En su opinión, “lo importante es saber seleccionar aquellas amenazas que son realmente críticas y contar con un equipo humano que pueda intervenir y bloquear este tipo de ataques”.

Inteligencia de amenazas, la mejor herramienta para anticiparse a los ataques

La investigación de amenazas constituye otro de los pilares de la estrategia de ESET. A través del seguimiento continuo de campañas maliciosas, grupos de ciberdelincuentes e indicadores de compromiso, la compañía proporciona a las organizaciones el contexto necesario para comprender cómo evolucionan los ataques y qué medidas deben adoptar para protegerse. “Hay que unir las diferentes piezas del puzle para que las empresas entiendan lo que está ocurriendo y sepan cómo protegerse”, asegura. Esa inteligencia también permite identificar puntos débiles antes de que sean explotados y compartir información con empresas, organismos públicos y fuerzas de seguridad para contribuir a la detección y desarticulación de campañas criminales.

> “Hay que saber a qué nos enfrentamos para poder preparar nuestras defensas”

Josep Albors, responsable de Investigación y Concienciación de **ESET,**

Además de reforzar sus soluciones de protección multicapa con inteligencia artificial, ESET prepara una inversión de 40 millones de euros para desarrollar una plataforma propia de IA en suelo europeo. Según explica Albors, esta iniciativa permitirá reforzar tanto la soberanía tecnológica como la disponibilidad de capacidades críticas para la defensa, reduciendo la dependencia de proveedores externos en un contexto geopolítico cada vez más incierto. “No podemos depender de que alguien decida que esas herramientas dejan de estar disponibles”, afirma, aludiendo a la importancia de garantizar el acceso a tecnologías estratégicas para la protección de las organizaciones europeas.

De cara a los próximos años, Josep Albors identifica una prioridad clara: reforzar la inteligencia de amenazas. Considera que conocer cómo actúan los atacantes permite optimizar las inversiones, proteger los activos realmente críticos y aprovechar mucho mejor las capacidades de las herramientas de seguridad. Muchas organizaciones, explica, incorporan nuevas soluciones convencidas de que ya están protegidas, cuando en realidad desconocen los riesgos a los que se enfrentan o no cuentan con los recursos necesarios para sacar partido a esas tecnologías. “Hay que saber a qué nos enfrentamos para poder preparar nuestras defensas”, afirma. En un escenario marcado por la automatización, los agentes de IA y campañas cada vez más rápidas, disponer de esa inteligencia será, en su opinión, uno de los factores que marcarán la diferencia entre reaccionar tarde o anticiparse a los ataques.

Kaspersky: “Un dato sin contexto no sirve absolutamente de nada”

Para Óscar Suela, Country Manager de Kaspersky Iberia, la ciberresiliencia ha dejado de medirse únicamente por la capacidad de evitar ataques. Las organizaciones asumen ya que tarde o temprano sufrirán un incidente y, por tanto, el verdadero reto consiste en anticiparse, responder con rapidez y aprender de cada ataque para fortalecer sus defensas. A este planteamiento se suma un nuevo factor: la continuidad de negocio. “Las organizaciones ya no solo están mirando el nivel de seguridad; también están empezando a mirar el nivel de continuidad de negocio”, explica. La cuestión ya no es únicamente impedir un compromiso, sino garantizar que la actividad pueda mantenerse incluso bajo ataque.

Rosalía Arroyo

Óscar Suela,
Country Manager de K**Kaspersky** Iberia,

El principal desafío para conseguirlo, en su opinión, es la velocidad a la que cambia el entorno tecnológico. La incorporación constante de servicios cloud, aplicaciones SaaS, herramientas de inteligencia artificial y nuevos proveedores hace que la superficie de exposición evolucione mucho más deprisa que las evaluaciones tradicionales de riesgo. “Ya no vale con hacer evaluaciones periódicas de seguridad”, advierte. Lo que una organización revisó hace apenas unas semanas puede haber cambiado completamente, obligando a adoptar modelos de evaluación y monitorización mucho más continuos.

La continuidad del negocio redefine el concepto de ciberresiliencia.

Desde la perspectiva de Kaspersky, ese cambio también se refleja en la evolución del propio cibercrimen. Los atacantes funcionan cada vez más como organizaciones empresariales que buscan maximizar la rentabilidad de sus operaciones. Según explica Suela, el ransomware ha evolucionado hacia modelos donde el verdade-

> “Las organizaciones ya no sólo están mirando el nivel de seguridad; también están empezando a mirar el nivel de continuidad de negocio”

ro valor ya no reside únicamente en cifrar la información, sino en obtener acceso a los datos y monetizarlos posteriormente. “El ransomware es hoy mucho más ransom que ware”, resume. Dentro de esa profesionalización cobran especial protagonismo los Initial Access Brokers, grupos especializados en conseguir un primer acceso a las organizaciones para vender posteriormente ese punto de entrada a otros delincuentes, reduciendo costes y acelerando las campañas.

La inteligencia artificial está contribuyendo a acelerar todavía más esta evolución. Suela evita hacer predicciones a largo plazo, pero sí observa tendencias que ya están transformando el panorama actual. La automatización permite lanzar campañas más numerosas y personalizadas, mientras que tecnologías como los modelos generativos dificultan distinguir entre elementos legítimos y maliciosos. Incluso anticipa un escenario en el que aparecerán auténticos “gemelos digitales maliciosos” (Evil Security Twin), capaces de replicar infraestructuras o dispositivos con un grado de realismo suficiente para engañar tanto a usuarios como a organizaciones.

La inteligencia de amenazas aporta el contexto necesario para responder antes

Frente a este escenario, la inteligencia de amenazas adquiere un papel decisivo. Para Suela, disponer de información no basta si no va acompañada del contexto adecuado. “Un dato sin contexto no sirve absolutamente de nada”, afirma. La inteligencia permite atribuir una amenaza a un actor concreto, comprender las tác-

> “La diferencia la marcará la rapidez para detectar un incidente y la eficiencia con la que se responda”

Óscar Suela, Country Manager de K**Kaspersky** Iberia,

ticas empleadas, conocer cómo responder y reducir significativamente los tiempos de reacción. Esa capacidad para contextualizar un incidente convierte la inteligencia de amenazas en una ventaja competitiva para acelerar tanto la detección como la respuesta.

La propuesta de Kaspersky combina esa capacidad de investigación con la incorporación de inteligencia artificial en sus propias tecnologías de protección. La compañía lleva años utilizando modelos de machine learning para mejorar la detección de amenazas y ha reforzado recientemente esta estrategia con un centro de excelencia especializado en inteligencia artificial. Además de mejorar sus capacidades defensivas, este equipo ayuda a las organizaciones a desarrollar modelos de IA seguros, evaluar su comportamiento, verificar su cumplimiento normativo y analizar cómo los ciberdelincuentes están aprovechando estas tecnologías para perfeccionar sus ataques.

De cara a los próximos años, Suela considera que la capacidad de detección y respuesta seguirá siendo el principal factor diferenciador entre las organizaciones más resilientes y las más vulnerables. La clave estará en disponer de monitorización en tiempo real, inteligencia de amenazas actualizada y mecanismos capaces de adaptar continuamente las defensas a la evolución de las tácticas, técnicas y procedimientos utilizados por los atacantes. “La diferencia la marcará cómo de rápido seas capaz de detectar un incidente y cómo de eficiente seas en la respuesta”, concluye.

SonicWall: “Hay que modernizar el acceso remoto y avanzar hacia Zero Trust”

La mayor complejidad de las infraestructuras tecnológicas, la desaparición del perímetro y el uso de la inteligencia artificial están obligando a las organizaciones a replantear su estrategia de ciberseguridad. Para Sergio Martínez, Regional Sales Manager de SonicWall Iberia, el verdadero reto ya no consiste en impedir que se produzca un ataque, sino en ser capaces de detectarlo con rapidez y responder sin comprometer la continuidad del negocio.

Rosalía Arroyo

Sergio Martínez,
Regional Sales Manager de **SonicWall** Iberia

“La realidad es que todas las organizaciones están y van a sufrir todo tipo de ataques”, afirma el directivo, añadiendo que, a su juicio, la diferencia estará en la capacidad para reaccionar ante incidentes que, en muchas ocasiones, permanecen ocultos durante meses. “La ciberresiliencia al final es esa capacidad que tienen las organizaciones para darse cuenta de lo que está pasando y poder reaccionar para seguir manteniendo el negocio en marcha”, resume. Un objetivo que, reconoce, resulta cada vez más complejo por la sobrecarga de alertas que reciben los equipos de seguridad y por la dificultad para distinguir cuáles requieren una actuación inmediata.

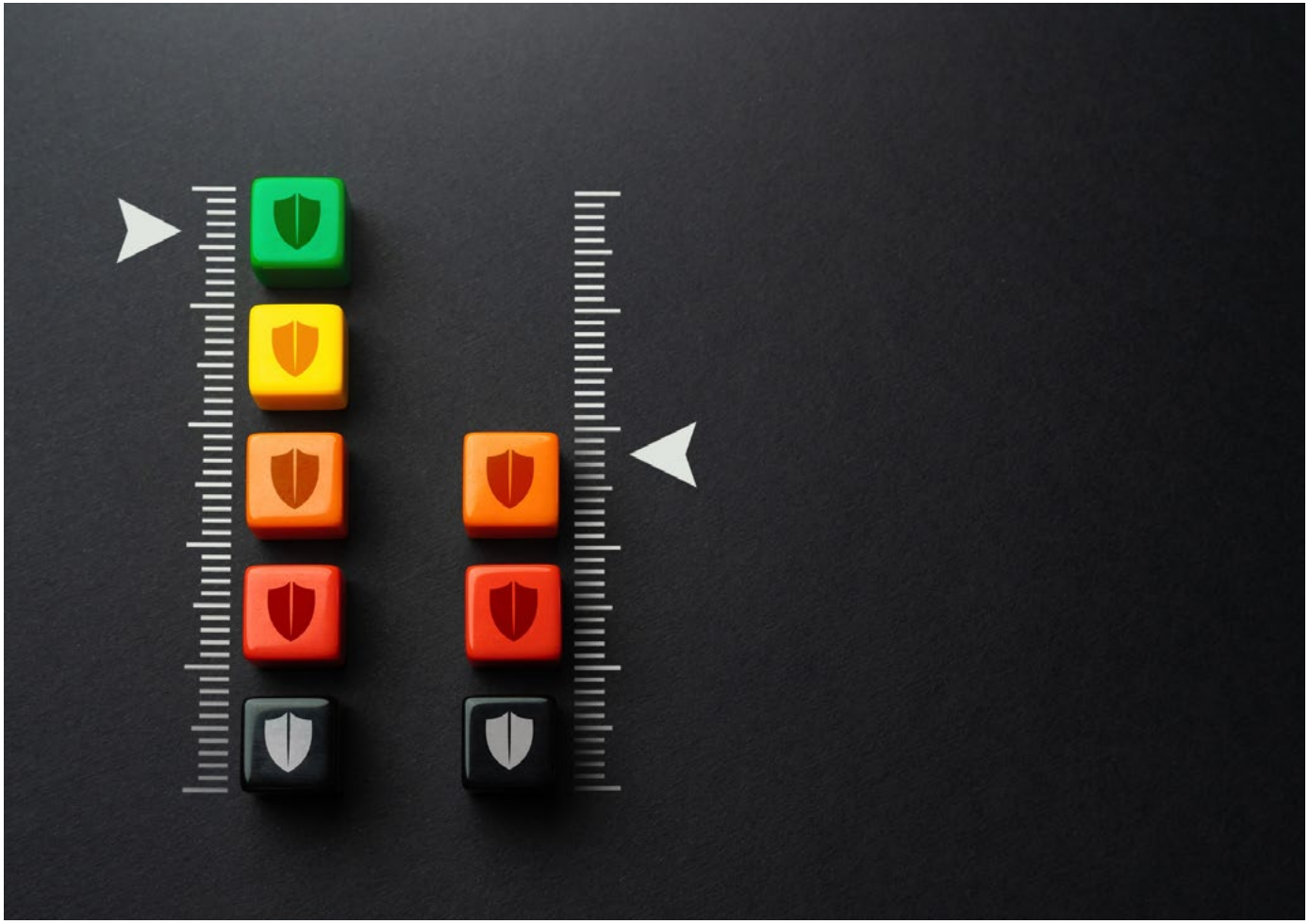
La identidad y el acceso remoto, en el centro del riesgo

Sergio Martínez considera que esa complejidad responde a varios factores. Las redes son más distribuidas, los empleados trabajan desde cualquier lugar y el concepto de perímetro ha dado paso a un modelo en el que la identidad se ha convertido en el principal objetivo de los atacantes. “El 85 % de las alertas tiene que ver con in-

> “La ciberresiliencia consiste en darse cuenta de lo que está pasando y poder reaccionar para seguir manteniendo el negocio en marcha”

tentos de robo de identidad”, explica. A ello se suma la inteligencia artificial, que está proporcionando nuevas herramientas para localizar vulnerabilidades y automatizar ataques, lo que obliga a mantener una vigilancia permanente.

En este escenario, defiende que muchas organizaciones necesitan apoyarse en servicios de monitorización y SOC especializados. “No todas las organizaciones tienen gente vigilando su infraestructura 24 horas al día, siete días a la semana”, recuerda. Además, insiste en que el déficit de profesionales sigue siendo uno de los grandes desafíos del sector y que será necesario formar a más especialistas durante los próximos años.



El acceso remoto representa otro de los puntos críticos. Según Martínez, buena parte de las brechas de seguridad actuales están relacionadas con credenciales comprometidas, especialmente a través de conexiones VPN tradicionales. “La mitad de las filtraciones tienen que ver con credenciales de VPN comprometidas”, señala. Por ello, considera imprescindible avanzar hacia modelos Zero Trust, eliminar progresivamente el uso de SSL VPN y reforzar los mecanismos de autenticación multifactor para reducir la superficie de ataque.

> “La mitad de las filtraciones tienen que ver con credenciales de VPN comprometidas”

Sergio Martínez, Regional Sales Manager de **SonicWall** Iberia

Del firewall a una plataforma de servicios gestionados

Esta evolución del mercado también ha transformado la estrategia de SonicWall. Si durante años la compañía fue conocida principalmente por sus firewalls, hoy apuesta por una plataforma abierta capaz de integrar información procedente de múltiples tecnologías y ofrecer servicios avanzados de monitorización y respuesta. “Hemos pasado de una compañía de producto a una compañía de servicios”, afirma. El objetivo es proporcionar al canal las herramientas necesarias para construir servicios gestionados de seguridad sin tener que desplegar su propio SOC.

La inteligencia artificial desempeña un papel relevante dentro de esa estrategia. La compañía trabaja en SAMI, un asistente basado en IA integrado en su plataforma que permitirá correlacionar información procedente de endpoints, aplicaciones SaaS, redes y soluciones de distintos fabricantes para identificar incidentes con mayor rapidez y alertar a los partners cuando detecte una amenaza crítica.

A pesar de la constante evolución del panorama de amenazas, Martínez concluye con un mensaje que considera especialmente importante: las prioridades siguen siendo las mismas. “Siempre tenemos que hablar de lo mismo porque es lo mismo”, asegura al referirse a la autenticación multifactor, la aplicación de parches, la segmentación de redes, la monitorización continua o los planes de respuesta ante incidentes. “Son los basics de la ciberseguridad. Si todos fuéramos capaces de aplicar estos basics, igual podría decir aquello de que ya no todo va peor”.

Sophos: “La ciberresiliencia depende de que toda la seguridad funcione como un único sistema”

Para Álvaro Fernández, una organización verdaderamente ciberresiliente no es aquella que aspira a bloquear todos los ataques, sino la que está preparada para resistirlos, responder con rapidez y minimizar su impacto sobre el negocio.

Rosalía Arroyo

Durante años, explica, la ciberseguridad se ha entendido como una suma de productos independientes —protección del puesto de trabajo, firewall, correo electrónico, identidad o nube—, pero el escenario actual exige un planteamiento diferente. “La resiliencia hoy depende de que todas esas capacidades funcionen como un sistema, no como piezas aisladas”, asegura. La ciberresiliencia ha dejado de ser una cuestión puramente técnica para convertirse en una capacidad operativa que combina tecnología, procesos, inteligencia de amenazas, automatización y experiencia humana.

La fragmentación de las herramientas debilita la capacidad de respuesta

En su opinión, el principal obstáculo ya no es la falta de herramientas. De hecho, muchas organizaciones cuentan con más soluciones de seguridad que nunca. El verdadero problema aparece cuando esas tecnologías funcionan de forma independiente, generan miles de alertas inconexas y obligan a los equipos a reconstruir manualmente el contexto de cada incidente. “La gran brecha está entre tener la tecnología y conseguir que esa tecnología funcione como un sistema”, resume. A ello se suman la falta de tiempo, la escasez de profesionales especializados y la dificultad para mantener una vigilancia permanente, factores que Sophos identifica como la “línea de pobreza de la ciberseguridad”: el punto en el que una organización ya no dispone de los recursos necesarios para defenderse con garantías frente a un panorama de

Álvaro Fernández,
director de ventas en **Sophos** Iberia

> “La IA debe multiplicar al experto, no sustituir su criterio”

amenazas que evoluciona a velocidad máquina. Ese escenario se agrava a medida que los atacantes reducen los tiempos necesarios para comprometer una organización. Mientras los ciberdelincuentes automatizan sus operaciones y utilizan inteligencia artificial para acelerar sus campañas, muchos equipos de seguridad siguen respondiendo manualmente, revisando alertas dispersas entre diferentes consolas e intentando reconstruir lo sucedido cuando el ataque ya está en marcha. Fernández considera que esa asimetría solo puede corregirse mediante una mayor integración entre tecnologías, automatización de tareas repetitivas y una mejor contextualización de la información. En su opinión, “no se trata de sustituir al analista, sino de darle un punto de partida mucho mejor”. La consolidación de capacidades también está transformando la forma en que las organizaciones abordan la ciberresiliencia. Según Fernández, cada vez son menos las empresas que pueden permitirse construir y mantener un SOC propio con cobertura permanente. En su lugar, el mercado evoluciona hacia modelos donde las capacidades avanzadas de detección y respuesta se consumen como un servicio, apoyándose en tecnología, procesos y expertos externos. En este contexto, el MDR deja de ser únicamente un servicio de monitorización para convertirse en una capacidad operativa que combina inteligencia, automatización y criterio humano. “Los clientes no compran solo una herramienta; compran confianza. Quieren saber que, si ocurre algo a las tres de la mañana, habrá alguien capaz de detectarlo, entenderlo y contenerlo”, señala.

IA, automatización y MDR para construir un sistema de defensa conectado

Esta visión también se refleja en la evolución de la propuesta de Sophos con Sophos Fusion,

una arquitectura abierta y nativa de inteligencia artificial que busca unificar la telemetría procedente de diferentes productos y transformar múltiples señales aisladas en una respuesta coordinada. El objetivo no es añadir otra consola de gestión, sino crear un contexto común que permita correlacionar eventos, automatizar actuaciones y acelerar la toma de decisiones. “No tener más herramientas, sino conseguir que la defensa actúe de forma conectada, inteligente y continua”, resume.

En ese modelo, la inteligencia artificial desempeña un papel protagonista, aunque Fernández insiste en que debe entenderse como una herramienta al servicio de las personas. “La IA debe multiplicar al experto, no sustituir su criterio”, afirma. La automatización permite correlacionar eventos, enriquecer el contexto, realizar investigaciones iniciales y ejecutar determinadas respuestas, pero las decisiones críticas siguen dependiendo del juicio de los analistas. “La IA aporta escala y velocidad, pero las personas aportan la experiencia, el criterio y la responsabilidad”, explica. Sólo cuando ambas trabajan conjuntamente dentro de una arquitectura común es posible mejorar de forma estructural la capacidad de respuesta.

Álvaro Fernández, director de ventas en **Sophos** Iberia

De cara a los próximos años, Fernández considera que la capacidad de detección y respuesta seguirá marcando la diferencia entre las organizaciones más resilientes y las más vulnerables. La prevención continuará siendo necesaria, pero resultará insuficiente frente a amenazas cada vez más rápidas, automatizadas y apoyadas en inteligencia artificial. Asegura que “la diferencia estará en detectar antes, entender mejor y responder con más coordinación”, y que para lograrlo, las organizaciones deberán abandonar los silos tecnológicos y evolucionar hacia modelos donde la tecnología, la inteligencia artificial y la inteligencia de amenazas funcionen como un único sistema de defensa.

Utimaco: “Las claves criptográficas son uno de los principales puntos ciegos de la ciberresiliencia”

Durante años, la ciberresiliencia estuvo ligada a la capacidad de recuperarse tras un incidente. Sin embargo, Jordi García ingeniero senior de preventa de Utimaco, considera que esa visión ha quedado superada. “Una empresa ciberresiliente debería ser capaz de seguir prestando sus servicios esenciales incluso bajo ataque”, afirma el directivo, explicando que, para conseguirlo ya no basta con disponer de copias de seguridad o planes de contingencia.

Rosalía Arroyo

Jordi García,
ingeniero senior de preventa de **Utimaco**

También es necesario diseñar arquitecturas preparadas para ser comprometidas, establecer mecanismos de gobernanza que permitan tomar decisiones con rapidez y fomentar una cultura en la que la seguridad forme parte del ADN de toda la organización.

En su opinión, varios factores están acelerando esta transformación. La creciente interdependencia entre organizaciones, proveedores cloud y cadenas de suministro hace que un incidente deje de ser un problema aislado para convertirse en un riesgo compartido. A ello se suma una presión regulatoria cada vez mayor, impulsada por normas como NIS2, DORA o el Reglamento de Ciberresiliencia, y una digitalización que reduce al mínimo la tolerancia a cualquier interrupción del servicio. “Cuanta más digitalización, menos tolerancia a una caída de servicio”, resume.

La confianza digital exige mucho más que continuidad de negocio

La inteligencia artificial añade una nueva dimensión al problema. Más allá de facilitar ataques más sofisticados, Jordi García considera que está

> “Una empresa ciberresiliente debería ser capaz de seguir prestando sus servicios esenciales incluso bajo ataque”

desplazando parte del foco desde la confidencialidad hacia la autenticidad y la integridad de los datos. Si un modelo de IA toma decisiones basándose en información alterada o manipulada, las consecuencias pueden ser críticas para el negocio sin que exista necesariamente una fuga de información. Explica el directivo que “el reto es determinar si esos datos son realmente fiables, si provienen de una fuente auténtica o si han sido alterados”. En ese escenario, la criptografía, la firma digital y los certificados adquieren un papel decisivo para garantizar la confianza sobre la que operan los sistemas de IA.

Precisamente, el especialista de Utimaco considera que la gestión de claves criptográficas y certificados continúa siendo uno de los aspectos más infravalorados de la ciberresiliencia, asegurando que “las claves criptográficas y los certificados son como la electricidad. Nadie se da cuenta de que están ahí hasta que cae el suministro”. De ellos dependen la autenticación de usuarios, el cifrado de las comunicaciones, la firma de código o la validación de actualizaciones de software, por lo que una mala gestión de su ciclo de vida puede provocar la interrupción de servicios críticos incluso sin que exista un ciberataque.

Esta realidad también está estrechamente relacionada con el creciente interés por la soberanía digital. Para Jordi García, no basta con conocer dónde se almacenan los datos. Lo verdaderamente importante es quién controla las claves criptográficas que los protegen. “De nada sirve que los datos estén en territorio europeo si las claves están bajo el control de un proveedor su-

> “Las claves criptográficas y los certificados son como la electricidad: nadie se da cuenta de que están ahí hasta que cae el suministro”

Jordi García, ingeniero senior de preventa de **Utimaco**

jeto a otra jurisdicción”, asegura. En su opinión, la confianza digital y la soberanía deben evolucionar conjuntamente para garantizar un control efectivo sobre la información.

Criptografía y soberanía, claves para la era poscuántica

Desde esa perspectiva, Utimaco centra su propuesta de valor en la protección de los activos criptográficos mediante módulos hardware de seguridad (HSM), capaces de generar y custodiar claves criptográficas y ejecutar operaciones de firma o cifrado dentro de un entorno seguro. Unas capacidades que, según explica, resultarán cada vez más importantes a medida que la inteligencia artificial se incorpore a procesos críticos y las organizaciones necesiten garantizar la integridad y autenticidad tanto de los modelos como de los datos que utilizan.

La computación cuántica representa el siguiente gran desafío. Jordi García reconoce que hace apenas un año muchas organizaciones todavía percibían esta amenaza como algo lejano, pero asegura que la situación ha cambiado de forma significativa. El riesgo de “almacenar ahora para descifrar después” y la aparición de algoritmos criptográficos poscuánticos están impulsando los primeros proyectos de transición. No obstante, advierte de que muchas empresas aún desconocen dónde se encuentran realmente sus claves y certificados, un paso imprescindible para afrontar esa migración con garantías. “La concienciación está ahí y eso me alegra”, concluye.

WatchGuard: “La fatiga operativa es hoy uno de los principales riesgos para la ciberresiliencia”

“Una organización verdaderamente ciberresiliente es aquella que asume que puede sufrir un incidente y que se prepara para continuar operando incluso durante ese incidente”, segura Jorge Pages, ingeniero preventa en el área de Cuentas Estratégicas de WatchGuard, para añadir que, en su opinión, la diferencia ya no la marca únicamente la capacidad para evitar un ataque, sino la rapidez con la que una organización es capaz de detectarlo, contenerlo y recuperar la actividad.

Rosalía Arroyo

Jorge Pages, ingeniero preventa en el área de Cuentas Estratégicas de **WatchGuard**

Para ello resulta imprescindible combinar visibilidad, detección temprana, procedimientos de respuesta bien definidos y una implicación que trascienda el departamento de TI para involucrar también a la dirección y al negocio.

La complejidad también es un riesgo para la ciberresiliencia

El especialista de WatchGuard cree que el principal desafío al que se enfrentan hoy las organizaciones es la velocidad con la que evoluciona la superficie de ataque. A la complejidad, se suma la escasez de profesionales especializados, que dificulta la monitorización continua y la respuesta ante incidentes. “El reto ya no es únicamente incorporar más tecnología, sino conseguir que esa tecnología, los procesos y las personas trabajen coordinados para adaptarse a un entorno en constante cambio”, resume.

Precisamente esa complejidad está provocando una situación paradójica. Las organizaciones disponen hoy de más herramientas de segu-

> “La pregunta ya no es si una organización va a sufrir un intento de ataque, sino cuánto tiempo va a tardar en detectarlo, contenerlo y volver a su actividad normal”

ridad que nunca, pero los equipos tienen cada vez más dificultades para gestionarlas. El elevado volumen de alertas, la presión operativa y la necesidad de tomar decisiones en muy poco tiempo incrementan el riesgo de que una amenaza relevante pase desapercibida o de que la respuesta llegue demasiado tarde. Tiene claro el directivo de WatchGuard que “la fatiga operativa es hoy uno de los principales riesgos para la ciberresiliencia”, al tiempo que considera que las organizaciones más maduras no son necesariamente las que acumulan un mayor número de soluciones, sino aquellas que consiguen simplificar la operación, automatizar tareas y concentrar sus esfuerzos en los riesgos que realmente afectan al negocio.

Plataformas integradas y MDR para hacer más con los mismos recursos

En este contexto, la consolidación de plataformas se está convirtiendo en una necesidad más que en una decisión de optimización. Tras años incorporando herramientas específicas para resolver problemas concretos, muchas organizaciones se encuentran ahora con múltiples consolas, políticas y procesos difíciles de coordinar. Pages subraya que consolidar no implica necesariamente trabajar con un único proveedor, sino conseguir que las diferentes tecnologías compartan información y proporcionen una visión coherente del riesgo. “La consolidación está dejando de ser

una cuestión de optimización y se convierte en algo clave para operar la seguridad de forma sostenible a largo plazo", explica.

WatchGuard lleva años apostando por este modelo mediante una plataforma unificada que integra diferentes capacidades de protección, automatización y correlación de eventos. Según Pages, este enfoque resulta especialmente útil para aquellas organizaciones que cuentan con equipos reducidos y deben gestionar infraestructuras, redes y seguridad con los mismos recursos. La integración, la visibilidad centralizada y la automatización permiten reducir la carga operativa y dedicar más tiempo a aquellas tareas que realmente aportan valor al negocio.

Ese mismo objetivo explica el creciente protagonismo de los servicios MDR. Aunque recuerda que el concepto no es nuevo y que tradicionalmente estaba reservado a grandes organizaciones con un SOC propio, considera que hoy responde a una necesidad mucho más amplia. Asegura durante la entrevista que "el verdadero valor del MDR no es detectar más amenazas, sino responder antes a las que realmente importan" y defiende un modelo que combine la monitorización

Jorge Pages, ingeniero preventa en el área de Cuentas Estratégicas de **WatchGuard**

continua, la automatización y el trabajo de analistas especializados capaces de aportar criterio y priorizar los incidentes con mayor impacto para el negocio.

De cara a los próximos años, Pages cree que la capacidad de detección y respuesta marcará la diferencia entre las organizaciones más resilientes y las más vulnerables. La prevención seguirá siendo necesaria, pero el incremento de ataques automatizados y el uso de inteligencia artificial obligarán a reforzar la capacidad para identificar comportamientos anómalos, contener rápidamente los incidentes y minimizar su impacto sobre la actividad. "La ciberresiliencia ya no consiste en construir muros más altos. Consiste en desarrollar la capacidad de adaptarse, responder y seguir operando en un entorno donde las amenazas son inevitables", concluye.