

OBSERVATORIO TAI CIBERRESILIENCIA

**Ciberresiliencia: del “evitar incidentes”
al “seguir operando bajo ataque”**



Ciberresiliencia: del “evitar incidentes” al “seguir operando bajo ataque”

Durante años, la ciberseguridad se centró en evitar los ataques, confiando en firewalls, antivirus y sistemas de detección para mantener a raya a los adversarios. Sin embargo, la realidad actual ha demostrado que los ciberataques son inevitables: las superficies de exposición crecen y las amenazas se vuelven más sofisticadas. Por eso, el objetivo ya no es blindarse por completo, sino garantizar la continuidad del negocio incluso bajo ataque.

Rosalía Arroyo

La ciberresiliencia se ha convertido en el nuevo estándar de madurez: un enfoque integral que combina prevención, resistencia, recuperación y evolución continua. Su meta no es eliminar el riesgo, sino gestionar su impacto, planificando la respuesta, automatizando procesos críticos y preparando a los equipos para mantener la ope-



rativa en condiciones adversas. Como resumen los expertos, “la diferencia entre una empresa atacada y una destruida está en su capacidad de recuperación”.

Este cambio de mentalidad se aceleró durante la pandemia, cuando la continuidad digital se

reveló esencial, y se consolidó con la creciente tensión geopolítica y la digitalización de los servicios esenciales. Hoy, la resiliencia no solo forma parte de las políticas de seguridad, sino también de la agenda económica y estratégica: la Unión Europea la ha situado en el centro de

sus programas de recuperación y regulaciones como NIS2 o DORA.

En el ámbito corporativo, medir la resiliencia se ha vuelto tan importante como medir la seguridad. Índices como el [Cyber Resilience Index](#) del Foro Económico Mundial evalúan la capacidad de una organización para seguir operando pese a una brecha. En definitiva, la ciberresiliencia amplía la visión de la ciberseguridad al integrar tecnología, gobernanza, gestión del riesgo y cultura organizativa, con un propósito claro: que las empresas resistan, aprendan y resurjan más fuertes tras cada incidente.

El ciclo de la ciberresiliencia

La ciberresiliencia se entiende como un proceso continuo compuesto por cuatro fases: Anticipar, Resistir, Recuperar y Evolucionar. Este ciclo busca que las organizaciones no solo se protejan, sino que también aprendan y mejoren tras cada incidente, reforzando su capacidad de adaptación.

1. Anticipar

La anticipación consiste en prepararse antes de que ocurra un ataque. Implica identificar

La ciberresiliencia no busca evitar lo inevitable, sino resistirlo y salir reforzado

riesgos, conocer las vulnerabilidades críticas y desarrollar mecanismos de alerta temprana. Las organizaciones que anticipan bien invierten en inteligencia de amenazas, realizan análisis de riesgos dinámicos y ejecutan simulacros periódicos de crisis o red teaming. También establecen políticas claras de resiliencia y revisan sus copias de seguridad y planes de contingencia. En la práctica, anticipar significa formar al personal, actualizar los escenarios de

Anticipar es preparar a la organización antes del impacto: el riesgo no avisa, pero sí se puede prever

riesgo y tener acuerdos con CERTs o expertos para responder rápido. Es, en definitiva, el paso de la reacción a la prevención proactiva.

2. Resistir

Por más que se planifique, los incidentes son inevitables. La fase de resistencia busca mantener las operaciones esenciales bajo ataque. Se basa en arquitecturas robustas, segmentación de redes, redundancia de sistemas y el modelo Zero Trust, que verifica continuamente identidades y accesos para frenar movimientos laterales de los atacantes. Tecnologías como EDR y XDR detectan comportamientos anómalos en tiempo real, mientras que infraestructuras redundantes y procedimientos de failover aseguran la continuidad. En este punto, resistir es sinónimo de absorber el golpe sin detener el negocio.

3. Recuperar

Cuando el incidente logra interrumpir servicios, entra en juego la recuperación, cuyo objetivo es restaurar la normalidad rápidamente. Combina herramientas técnicas —como copias inmutables o servicios de Disaster Recovery as a Service (DRaaS)— con una buena



planificación. La clave está en priorizar qué sistemas restaurar primero, validar que la restauración sea limpia (sin malware residual) y ejecutar el plan de continuidad previamente ensayado. Casos como el de Maersk tras NotPetya (2017) demuestran que una preparación sólida permite volver a operar en días. Recuperar, por tanto, es minimizar el impacto

económico y reputacional mientras se reanudan las funciones críticas.

4. Evolucionar (Adaptarse)

La última fase —a menudo la más olvidada— consiste en aprender del incidente. La resiliencia es un ciclo que mejora con cada iteración: se analizan fallos, se ajustan políticas y se actualizan procedimientos para elevar

la madurez. Las organizaciones más avanzadas documentan post-mortems detallados y aplican lecciones aprendidas a sus planes, tecnología y cultura. Incorporar inteligencia de amenazas actualizada y herramientas de automatización e IA refuerza la capacidad de adaptación. Un ejemplo son los SOC inteligentes, que correlacionan información global y reaccionan de forma casi autónoma.

Evolucionar implica aceptar que la seguridad perfecta no existe, pero la mejora continua sí. Cada ciclo refuerza la capacidad de anticipar mejor, resistir más tiempo y recuperarse más rápido. Así, la organización transforma cada incidente en una oportunidad de aprendizaje, avanzando hacia un estado de resiliencia madura y sostenida.

Tecnologías y estrategias clave para la ciberresiliencia

La ciberresiliencia no depende de una única solución, sino de un ecosistema integrado de tecnologías, procesos y personas que permiten anticipar, resistir y recuperarse de los ataques. Su objetivo no es evitar incidentes a toda costa,

Modelos y estándares internacionales de referencia

La ciberresiliencia se apoya en un conjunto de marcos internacionales y normativas que ofrecen un lenguaje común para construir y evaluar la capacidad de las organizaciones frente a incidentes. Entre ellos destaca el NIST Cybersecurity Framework (CSF), que articula cinco funciones —Identificar, Proteger, Detectar, Responder y Recuperar— alineadas con las fases de la resiliencia y propone niveles de madurez (de enfoque reactivo a adaptativo).

La norma ISO 22301 complementa este enfoque desde la continuidad de negocio, definiendo procesos, tiempos de recuperación y pruebas periódicas que institucionalizan la resiliencia. Por su parte, MITRE aporta una visión proactiva con su modelo de cuatro objetivos —Anticipar, Resistir, Recuperar y Evolucionar— y su matriz ATT&CK, referencia mundial para anticipar y contener ataques.

Otros marcos, como los CIS Controls, ofrecen una hoja de ruta táctica para reforzar las bases de la seguridad, mientras que ENISA impulsa la cooperación europea y la evaluación de la madurez sectorial. En el plano normativo, NIS2, DORA y el Esquema Nacional de Seguridad (ENS) obligan a incorporar planes de continuidad y gestión de riesgos, consolidando la resiliencia como requisito regulatorio. Incluso el futuro AI Act incluirá medidas para garantizar la robustez de los sistemas de inteligencia artificial, ampliando la resiliencia al corazón de la innovación digital.

sino garantizar la continuidad del negocio incluso en situaciones adversas.

Las plataformas de detección y respuesta avanzadas (XDR, EDR, SIEM, SOAR) son hoy el pilar

central de esta estrategia. Permiten identificar intrusiones, correlacionar señales en distintos entornos (nube, red, endpoints, identidades) y reaccionar con rapidez. Combinadas con inte-

ligencia artificial, filtran alertas, priorizan las críticas y automatizan tareas repetitivas. Las herramientas SOAR amplían esta capacidad: ante una amenaza confirmada, pueden aislar automáticamente un dispositivo, recopilar evidencias y restaurar sistemas, reduciendo drásticamente los tiempos de respuesta. En conjunto, XDR y SOAR forman la columna vertebral tecnológica de la resiliencia, al detectar antes, responder mejor y anticipar campañas de ataque mediante inteligencia global.

Otro elemento esencial es el control de identidades y el modelo Zero Trust, basado en el principio “nunca confiar, siempre verificar”. Cada acceso se valida continuamente, se aplican privilegios mínimos y se segmentan los entornos para impedir movimientos laterales. Tecnologías como ZTNA sustituyen a las VPN tradicionales, otorgando acceso solo a aplicaciones específicas. Con ello, las organizaciones reducen la superficie de ataque y los riesgos derivados del robo de credenciales, uno de los vectores más frecuentes.

En la fase de recuperación, el foco está en la continuidad operativa. Las soluciones de bac-

kup inmutable y la Recuperación ante Desastres como Servicio (DRaaS) garantizan que, ante un ransomware o una caída grave, los sistemas puedan restaurarse sin pagar rescates ni sufrir paradas prolongadas. Estas copias inmutables, almacenadas en entornos protegidos o en la nube, son inmunes a la manipulación o al borrado, y la replicación continua en infraestructuras alternativas permite reanudar la actividad casi al instante. A esto se suma la redundancia de sistemas —servidores en clúster, comunicaciones duplicadas, energía alternativa— y la obligación de probar regularmente estos mecanismos, porque un plan de recuperación sin ensayos reales es tan frágil como no tenerlo.

La automatización y la inteligencia artificial se consolidan como aceleradores de la resiliencia.

Cada incidente es una prueba de estrés para la organización... y una oportunidad de aprendizaje

Los algoritmos de aprendizaje automático detectan anomalías sutiles, incluso amenazas desconocidas (zero-day), y algunos sistemas ya ejecutan respuestas autónomas en milisegundos. Este enfoque, conocido como resiliencia autónoma, busca entornos capaces de autodefenderse y autorrepararse, reduciendo la dependencia humana en momentos críticos. Sin embargo, la IA también introduce nuevos riesgos —fraudes sintéticos, malware adaptativo, manipulación de modelos—, lo que obliga a equilibrar la automatización con la supervisión experta. La estrategia más eficaz será la que combine velocidad artificial con criterio humano.

Por encima de las herramientas, la cultura organizativa y el factor humano son los cimientos de una verdadera resiliencia. La formación y concienciación de los empleados, desde la base hasta la alta dirección, son esenciales para evitar errores y detectar amenazas. Empresas que realizan simulaciones periódicas de phishing o entrenamientos de crisis logran reducir drásticamente el impacto de incidentes. La gobernanza también es decisiva: la resiliencia debe

Resistir no es no caer, sino mantener el negocio en marcha incluso bajo ataque

ser un objetivo visible y medible, con apoyo de la dirección, integración en los cuadros de mando de riesgos y responsabilidades definidas para CISO, CIO y comités ejecutivos.

Finalmente, la gestión del talento se ha convertido en un reto global. Con dos de cada tres organizaciones afectadas por la falta de profesionales cualificados, resulta imprescindible fomentar la formación interna, retener al personal experto y, cuando sea necesario, apoyarse en servicios gestionados que refuercen las operaciones 24/7. Una cultura resiliente también implica colaboración transversal: seguridad, legal, comunicación, recursos humanos y dirección deben actuar coordinadamente ante un incidente.

En última instancia, la ciberresiliencia es tanto una actitud como una arquitectura. Implica asumir que los ataques ocurrirán y que lo impor-

tante no es evitarlos todos, sino responder con eficacia, aprender del impacto y salir reforzados. La tecnología proporciona la velocidad; las personas, la inteligencia y el propósito. Juntas, construyen la capacidad que diferencia a las organizaciones que simplemente sobreviven de aquellas que siguen operando y liderando incluso bajo ataque.

Desafíos actuales

A pesar de los avances en tecnología y conciencia, las organizaciones afrontan retos persistentes que condicionan su capacidad de ser verdaderamente resilientes. Tres destacan por su impacto: la escasez de talento, la complejidad tecnológica y la dependencia de terceros.

1. Falta de talento y sobrecarga de los equipos de seguridad.

La brecha de profesionales cualificados sigue siendo uno de los mayores obstáculos. La demanda crece mientras la oferta no cubre las necesidades, generando equipos sobrecargados, con alta rotación y menor capacidad de anticipación. Según el Foro Económico Mundial, solo el 14 % de las em-



presas confía plenamente en disponer del personal adecuado para gestionar sus riesgos cibernéticos. Para paliarlo, las organizaciones apuestan por la formación acelerada, la diversidad en la contratación, el refuerzo mediante servicios gestionados (MSSP/MDR) y el uso de IA para automatizar tareas rutinarias. Aun así, la falta de talento seguirá limitando la resiliencia a corto plazo, por lo que

planificarla debe incluir la gestión eficiente de los recursos humanos disponibles.

2. Complejidad tecnológica y exceso de herramientas.

La expansión del entorno digital —infraestructuras híbridas, IoT, trabajo remoto— ha multiplicado la complejidad y el número de soluciones de seguridad aisladas. Muchas empresas operan con decenas de herramientas que no

se comunican entre sí, dificultando la visibilidad y generando ineficiencias. La tendencia es hacia la consolidación e integración de plataformas, con arquitecturas más unificadas, automatizadas y fáciles de gestionar. También se busca simplificar la experiencia del usuario con enfoques como la autenticación sin contraseñas o la seguridad por diseño. En definitiva, la resiliencia tecnológica pasa por “menos es más”: entornos simplificados, interoperables y orquestados que respondan coordinadamente ante una crisis.

3. Dependencia de terceros y riesgo en la cadena de suministro.

La resiliencia ya no depende solo de la fortaleza interna, sino de todo el ecosistema digital. Los ataques a proveedores de software o servicios cloud —como SolarWinds o Kaseya— demostraron que una brecha en un tercero puede tener efectos en cascada. Normativas como DORA obligan a las entidades financieras a evaluar y supervisar el riesgo de sus proveedores TIC críticos. Cada vez más organizaciones incorporan evaluaciones de seguridad de terceros, planes de continuidad

compartidos y estrategias de diversificación para reducir dependencias. Paralelamente, la colaboración público-privada y el intercambio de inteligencia entre sectores —a través de

redes como EU-CyCLONE o la JCDC en EE. UU.— están configurando una resiliencia colectiva, donde la cooperación y la comunicación rápida se vuelven esenciales.

Modelos de madurez en ciberresiliencia

Evaluar qué tan preparada está una organización para resistir y recuperarse de un ataque es clave para mejorar su postura de seguridad. Los modelos de madurez en ciberresiliencia permiten medir ese nivel de preparación y definir una hoja de ruta hacia una mejora continua.

En Europa, el [Cyber Resilience Maturity Model \(CRMM\)](#) —impulsado por ENISA— analiza la resiliencia desde varias dimensiones: tecnología, procesos, personas y estrategia. Ayuda a identificar qué controles existen, su efectividad y las acciones necesarias para alcanzar el siguiente nivel. Así, una empresa puede pasar de ser reactiva a tener una capacidad planificada de respuesta y recuperación.

En Estados Unidos, el [Cyber Resilience Review \(CRR\)](#), desarrollado por el CERT y el Departamento de Seguridad Nacional, aplica el modelo CERT-RMM, basado en la filosofía CMMI, con cinco niveles de madurez: desde procesos ad hoc hasta un enfoque optimizado y de mejora continua.

Estos modelos —junto a marcos como NIST CSF— combinan indicadores cualitativos y cuantitativos, como tiempos medios de detección y respuesta (MTTD/MTTR), número de simulacros o nivel de automatización. Más allá de medir, su propósito es guiar inversiones, fomentar la mejora continua y convertir la resiliencia en una ventaja competitiva, alineando personas, procesos y tecnología bajo un mismo objetivo.

Los planes de contingencia son inútiles si no se prueban: la resiliencia se entrena, no se improvisa

En conjunto, el futuro de la ciberresiliencia dependerá tanto de la integración tecnológica como del factor humano y la cooperación intersectorial. Solo las organizaciones que logren coordinar estos tres ejes —personas, tecnología y ecosistema— podrán resistir, adaptarse y evolucionar frente a un entorno cada vez más incierto.

Tendencias futuras

El futuro de la ciberresiliencia estará marcado por tres grandes líneas de evolución: automatización inteligente, colaboración masiva y gobernanza sostenible.

1. Resiliencia autónoma y sistemas auto-reparables.

La inteligencia artificial y la automatización

avanzarán hacia entornos capaces de defenderse y repararse solos. Surgirán sistemas con respuesta automática ante ataques o fallos, capaces de aislar componentes comprometidos y restaurarlos sin intervención humana. Este enfoque, conocido como resiliencia autónoma, integrará analítica predictiva para anticipar fallos y reconfigurar dinámicamente la seguridad de red frente a amenazas. Aunque aún incipiente, la tendencia apunta a redes corporativas con una mayor inteligencia embebida y menor dependencia humana en crisis. El desafío será garantizar decisiones correctas y evitar manipulaciones de la IA por parte de atacantes.

2. Inteligencia colectiva y colaboración global.

La resiliencia se convertirá en un esfuerzo compartido. Las redes de intercambio de inteligencia en tiempo real entre empresas y organismos permitirán responder de forma coordinada ante nuevas amenazas. Gobiernos y entidades internacionales ya promueven simulacros conjuntos y marcos legales para facilitar esa cooperación. También crecerá la dimensión social de la resiliencia: edu-

cación ciudadana, cultura de “higiene digital” y colaboración interdisciplinar que integre factores humanos y psicológicos en la respuesta a cibercrisis.

3. Integración con ESG y confianza digital.

Cada vez más, la ciberresiliencia será vista como un indicador de buena gobernanza y sostenibilidad empresarial. Los criterios ESG incorporan ya la gestión del riesgo cibernético como parte de la responsabilidad corporativa. Inversores y clientes valorarán la transparencia y capacidad de recuperación de las empresas ante incidentes, y podrían surgir ratings públicos de resiliencia digital. En definitiva, la resiliencia dejará de ser un asunto técnico para consolidarse como un pilar estratégico y reputacional, esencial para

El modelo Zero Trust y la segmentación reducen el impacto del error humano y los movimientos laterales

Las copias inmutables y la recuperación como servicio marcan la frontera entre el caos y la continuidad

la supervivencia y la confianza en la economía digital.

Conclusión: el nuevo rostro de la seguridad digital


La transición de la ciberseguridad a la ciberresiliencia marca un cambio de paradigma: el éxito ya no se mide por los ataques evitados, sino por la capacidad de mantener el negocio en marcha y recuperarse con rapidez. Este enfoque no sustituye a la seguridad preventiva, sino que la amplía, aceptando que los incidentes son inevitables y que la verdadera fortaleza reside en la respuesta y la adaptación.

Adoptar la ciberresiliencia implica un cambio cultural profundo: pasar del “esto no nos pa-



sará” al “estamos preparados cuando ocurra”. Supone invertir en tecnología, pero también en personas, procesos y colaboración. Los consejos de dirección comienzan a comprender que la resiliencia equivale a continuidad del negocio y confianza, valores esenciales para accionistas, clientes y ciudadanos.

En el fondo, refleja la madurez del sector: de una visión defensiva a una estrategia proactiva

y antifrágil, donde cada incidente se convierte en aprendizaje. La ciberresiliencia será la piedra angular de la estrategia digital de esta década. Las organizaciones que integren este principio en su ADN no solo resistirán las tormentas, sino que convertirán esa capacidad en una ventaja competitiva. En un mundo donde el ataque es seguro, la diferencia está en cómo nos recuperamos. 

Automatización, IA y cultura corporativa: los tres pilares de la ciberresiliencia moderna

La ciberresiliencia ha dejado de ser una aspiración técnica para convertirse en una competencia esencial de negocio. En un entorno de amenazas constantes, las organizaciones más avanzadas combinan automatización, inteligencia artificial y una sólida cultura corporativa para anticiparse, resistir y recuperarse ante cualquier interrupción.

Rosalía Arroyo

La ciberresiliencia, una prioridad estratégica

La ciberresiliencia se ha convertido en uno de los ejes fundamentales de la estrategia tecnológica de las organizaciones españolas. Ya no se trata solo de resistir un ciberataque, sino de asegurar la continuidad del negocio, la recuperación rápida y la capacidad de adaptación ante cualquier interrupción, sea digital o física.

Para saber lo que está ocurriendo verdadera-



mente en el mercado, hemos contactado con varios responsables de TI y ciberseguridad de primer nivel. Los directivos que participan en este Observatorio de Ciberresiliencia son Josep Bardallo, CISO del Grupo Alimentario Ar-

gal, María Luisa Redondo Velázquez, Global Information Security Director en Horse; David Moreno el Cerro, CISO y CTO de Tendam; Guillermo Obispo San Román, Jefe del Servicio de Coordinación del Centro de Ciberseguridad del

Ayuntamiento de Madrid; y Ángel Gálvez, Global CISO de Dufry, quienes coinciden en que la resiliencia ya no es un asunto técnico, sino una competencia de negocio.

1. Medir la resiliencia: del control técnico al aprendizaje organizativo

“Lo más importante es la automatización de respuestas para casos conocidos y la reducción del factor humano en momentos de crisis”

Josep Bardallo,
CISO del Grupo Alimentario Argal

La primera cuestión que afrontan las compañías es cómo medir la ciberresiliencia de forma efectiva. Todos coinciden en que no existe un único indicador, sino un conjunto de métricas que combinan capacidad técnica, coordinación organizativa y aprendizaje.

Redondo explica que en Horse “se analizan los tiempos medios de detección y respuesta (MTTD/MTTR), el grado de cobertura de los sistemas críticos por los planes de continuidad y los resultados de los simulacros de ciberataques”. Bardallo añade que, en Argal, complementan estas métricas con un enfoque de madurez: “Además de los índices basados en NIST o ISO 27001, valoramos el porcentaje de controles automatizados y los resultados de los ejercicios frente a ransomware o caídas de proveedores”.

Desde el ámbito público, Obispo destaca que el Ayuntamiento de Madrid “mide su resiliencia a través del recuento de incidentes por tipología y del tiempo medio de respuesta”, pero insiste en que el verdadero avance se da cuando “una unidad mejora su detección temprana y logra limitar los recursos necesarios para contener un incidente”.

En el sector retail, David Moreno coincide en la importancia de probar la preparación de los equipos: “Evaluamos nuestra capacidad de recuperación a partir del RTO de los servicios críticos durante entrenamientos reales.

Es la forma más honesta de saber si estamos preparados”.

El consenso es claro: la ciberresiliencia se mide tanto por la rapidez con la que una organización se levanta tras un golpe como por lo que aprende en el proceso.

2. Tecnologías que refuerzan la capacidad de respuesta

Las tecnologías más eficaces son aquellas que permiten detectar antes, responder más rápido y recuperarse sin perder continuidad. En el entorno corporativo, soluciones como los sistemas EDR/XDR, las plataformas SIEM y los backups inmutables son ya estándares

“La concienciación ha pasado de ser un tema técnico a un riesgo estratégico empresarial”

María Luisa Redondo Velázquez,
Global Information Security Director enHorseL

consolidados. Redondo apunta que “las plataformas SOAR y las herramientas de gestión de vulnerabilidades nos permiten automatizar la respuesta y reducir la exposición antes de que ocurra un incidente”.

Bardallo coincide y subraya la importancia de reducir el margen de error humano: “Lo más importante es la automatización de respuestas para casos conocidos y la reducción del factor humano en momentos de crisis”.

En la administración madrileña, Obispo enfatiza el valor de la monitorización continua y la cooperación institucional: “Nuestra estrategia se apoya en la Red Nacional de SOCs y en la inteligencia de amenazas compartida con el CCN-CERT”.

Por su parte, Ángel Gálvez destaca la relevancia de las arquitecturas resilientes y distribuidas: “En Dufry utilizamos backups inmutables y mecanismos de alta disponibilidad entre regiones cloud. Esto nos permite recuperar la operativa en minutos incluso ante fallos eléctricos o ataques de ransomware”.

La conclusión es unánime: la tecnología es imprescindible, pero su eficacia depende de

la práctica, la automatización y la coordinación entre equipos.

3. La inteligencia artificial se abre paso

La inteligencia artificial ha comenzado a redefinir la gestión de amenazas, aportando capacidades predictivas y acelerando la toma de decisiones.

“La clave de la resiliencia está en mejorar la detección temprana y limitar los recursos necesarios para contener un incidente”

Guillermo Obispo San Román (Willy),
Jefe del Servicio de Coordinación del **Centro de Ciberseguridad del Ayuntamiento de Madrid**

Bardallo explica que su organización la aplica “en tres capas: análisis de comportamiento, modelos de scoring dinámico en identidad y, de forma incipiente, IA generativa para crear y validar playbooks o informes forenses”.

En Horse, María Luisa Redondo confirma que ya han integrado machine learning y análisis de comportamiento anómalo (UEBA) “para anticiparnos a ataques complejos y reducir tiempos de respuesta”.

Obispo reconoce que, en el Ayuntamiento de Madrid, “la mayoría de las soluciones de terceros ya incorporan IA, que ayuda a detectar patrones de ingeniería social o a optimizar la respuesta automatizada”.

David Moreno, desde Tendam, matiza que se encuentran en fase piloto: “Estamos explorando casos de uso, pero todavía no está desplegada de forma generalizada”.

El avance es desigual, pero la tendencia es clara: la inteligencia artificial está llamada a convertirse en el motor de la ciberresiliencia, no solo para detectar amenazas, sino también para documentar, aprender y anticipar comportamientos futuros.

4. Continuidad y recuperación: del plan al ejercicio

Tener un plan de continuidad no basta; hay que validarlo de forma continua.

Redondo detalla que en Horse “los planes de

continuidad y recuperación ante desastres incluyen procedimientos específicos ante ransomware y simulacros periódicos para garantizar que la respuesta funciona”.

Bardallo apunta que en Argal se ha dado un paso más: “Vinculamos los planes de continuidad (BCP) con escenarios de ciber crisis reales, incluyendo estrategias de comunicación con clientes y reguladores, prioridades por negocio y roles de liderazgo operativo definidos”.

En la administración pública, Obispo destaca que el Esquema Nacional de Seguridad

“Cada ejercicio nos enseña algo nuevo: la ciberresiliencia es un proceso continuo, no un objetivo final”

David Moreno el Cerro,
CISO y CTO de Tendam

y el Plan Territorial de Emergencia Municipal de Madrid ofrecen una base sólida, pero “la clave está en desarrollar nuevas capacidades de resiliencia digital y coordinación entre organismos”.

Moreno explica que en Tendam “la continuidad es uno de los escenarios más trabajados, tanto desde el plano técnico como desde el organizativo, con ejercicios tipo table-top que validan la toma de decisiones”.

Ángel Gálvez añade una perspectiva práctica: “Nuestro comité ejecutivo sitúa la seguridad y la recuperación como prioridades estratégicas. Los ejercicios con proveedores y la redundancia de servicios nos aseguran mantener la operativa incluso ante cortes eléctricos o incidentes globales”.

En todos los casos, la práctica continua y la integración entre negocio y tecnología son el verdadero termómetro de la preparación corporativa.

5. NIS2 y DORA: catalizadores del cambio

Las normativas europeas NIS2 y DORA están impulsando la profesionalización de la ciberresiliencia, al obligar a reforzar la go-

“La resiliencia ya forma parte del ADN corporativo; es una responsabilidad compartida entre todas las áreas del negocio”

Ángel Gálvez,
Global CISO de Dufry

bernanza y la supervisión de la cadena de suministro.

“Ambas normas han obligado a formalizar la resiliencia como responsabilidad del órgano de dirección y a reforzar el control sobre terceros”, señala Bardallo. “Nos sirven como catalizador para conseguir apoyos y presupuesto”.

María Luisa Redondo confirma que su impacto se siente también en el ámbito corporativo: “Han fortalecido los mecanismos de reporte, la gobernanza directiva y los controles técnicos y organizativos, incluyendo auditorías más frecuentes”.

Obispo recuerda que, en el sector público, “NIS2 refuerza la aplicación del ENS y amplía la supervisión sobre entidades críticas”.

Aunque Tendam no está directamente sujeta a estas normativas, Moreno admite que “sus principios sirven como referencia de buenas prácticas que aplicamos voluntariamente”.

En conjunto, estas regulaciones han elevado el estándar de resiliencia exigido en todos los sectores y han acelerado la madurez del diálogo entre tecnología y dirección.

6. La dirección, más consciente y comprometida

El cambio cultural es, quizá, el más significativo. Todos los entrevistados coinciden en que la alta dirección ha pasado de la indiferencia a la implicación activa.

“Ya no preguntan por qué invertir en resiliencia, sino cómo estamos respecto al sector”, resume Bardallo. Redondo destaca que en Horse “la ciberresiliencia está integrada en la agenda estratégica, con participación del comité de dirección en simulacros y ejercicios de crisis”.

Moreno afirma que en Tendam “la dirección



lleva años impulsando una cultura de ciberseguridad e invirtiendo en capacidades que aseguren una recuperación ágil y con mínimo impacto”.

Obispo subraya que en el Ayuntamiento de Madrid “la dirección respalda campañas de concienciación y participa directamente en los ejercicios de contingencia”.

Y Gálvez lo resume con claridad: “La resiliencia


ya forma parte del ADN corporativo. Es una responsabilidad compartida entre todas las áreas del negocio”.

La ciberresiliencia ha pasado de ser un asunto técnico a un compromiso transversal y estratégico.

La resiliencia como ventaja competitiva

El análisis de las visiones de estos CISO y responsables públicos evidencia una evolución significativa: la ciberresiliencia ya no es un objetivo, sino un proceso continuo de adaptación. Las organizaciones más avanzadas combinan automatización, inteligencia artificial y entrenamiento constante. La regulación europea actúa como motor de madurez y la cultura corporativa se consolida como el factor diferencial.

Como señala María Luisa Redondo, “la concienciación ha pasado de ser un tema técnico a un riesgo estratégico empresarial”.

El futuro apunta hacia una resiliencia predictiva, capaz de anticipar no solo los ataques, sino también las interrupciones operativas. O, como concluye Bardallo, “la resiliencia no es resistir, es adaptarse más rápido que los demás”. 

Check Point: “Las arquitecturas homogéneas son clave para alcanzar una resiliencia real”

La ciberresiliencia está redefiniendo las prioridades tecnológicas de las organizaciones. Ya no basta con prevenir un ataque: hay que ser capaz de recuperarse y seguir operando con rapidez. Así lo asegura Eusebio Nieva, director técnico de Check Point Iberia, quien defiende que la simplicidad, la automatización y las arquitecturas coherentes son las verdaderas bases de una defensa resiliente y sostenible.

Rosalía Arroyo

Nieva reconoce que muchas compañías han avanzado en prevención, pero siguen mostrando carencias críticas en recuperación y continuidad. “Todo el mundo planifica el backup, pero pocos planifican la recuperación”, comenta. Un error común que, según él, convierte los incidentes en crisis prolongadas.

El directivo explica que la mayoría de las estrategias de ciberseguridad se diseñan desde una lógica reactiva: se invierte después del incidente, no antes. “Las empresas que más sufren no son las que han sido atacadas, sino las que no habían probado sus planes de contingencia”,

“Todo el mundo planifica el backup, pero pocos planifican la recuperación”

advierde. Para él, la resiliencia no es una herramienta, sino un proceso continuo de anticipación, validación y aprendizaje.

En este sentido, la normativa NIS2 está sirviendo de punto de inflexión. “Por primera vez, se exige que las organizaciones documenten, prueben y supervisen sus planes de respues-



Eusebio Nieva, director técnico de Check Point Iberia

ta. Ya no es opcional, es un requisito”, subraya Eusebio Nieva. Esa obligación regulatoria, añade, está impulsando una cultura más madura,

donde la seguridad se percibe como un factor estratégico y no solo técnico.

Antes, durante y después: la visión de Check Point

Check Point estructura su enfoque de ciberresiliencia en tres fases: antes, durante y después del ataque.

En la primera, la compañía garantiza que sus tecnologías lleguen al cliente “listas para operar de forma segura”. Esto implica incorporar medidas de protección nativas desde el diseño y reducir la dependencia de actualizaciones o parches continuos. “Las empresas no pueden permitirse una seguridad improvisada. La protección tiene que venir integrada”, explica Nieva.

Durante un ataque, la prioridad es la visibilidad y la coordinación. La plataforma unificada de Check Point ofrece una vista centralizada de toda la infraestructura —nube, red, endpoints y usuarios—, lo que permite a los equipos detectar anomalías, priorizar alertas y orquestar respuestas automáticas. “Una organización que ve lo que pasa, controla la situación. La que no ve, reacciona tarde”, resume el directivo.



Finalmente, en la etapa posterior, el acompañamiento es clave. Check Point ayuda a las empresas a analizar la causa raíz, revisar la configuración y reforzar procedimientos.

Identidad, automatización y control en un perímetro multiplicado

El perímetro, señala Nieva, “no ha desaparecido; se ha multiplicado”. Las redes híbridas, el trabajo remoto y el crecimiento del cloud han fragmentado la superficie de exposición. Cada usuario, servicio o aplicación representa un nuevo punto de acceso que puede ser explota-

do si no se controla adecuadamente.

En este contexto, la automatización y la inteligencia artificial (IA) se han convertido en pilares esenciales de la defensa moderna. “Las defensas deben ser lo suficientemente autónomas e inteligentes como para responder sin errores”, sostiene. Check Point utiliza IA y machine learning para detectar patrones de comportamiento anómalos, reducir los falsos positivos y ejecutar acciones inmediatas ante una amenaza.

Sin embargo, Nieva matiza que la automatización no debe sustituir la toma de decisiones humanas. “La tecnología acelera, pero el criterio

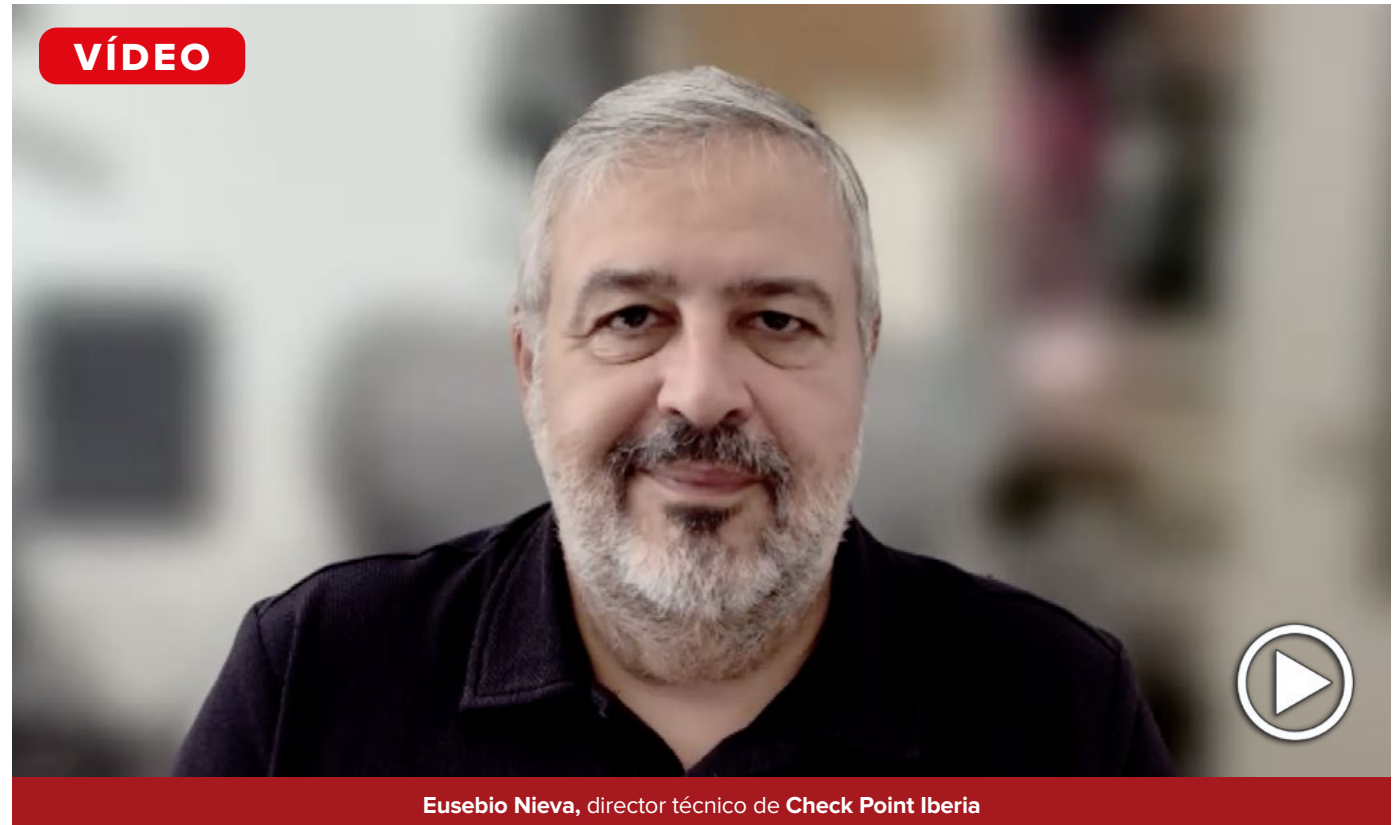
lo pone la persona. La clave está en equilibrar velocidad y precisión”, señala.

Arquitecturas homogéneas para una resiliencia real

Considera Eusebio Nieva que la consolidación tecnológica es la gran asignatura pendiente de las empresas. “Cuanta más complejidad, menos visibilidad y control”, resume, añadiendo que las organizaciones han acumulado múltiples herramientas sin una estrategia unificada, lo que genera redundancias, lagunas y sobrecostos.

Su recomendación es avanzar hacia arquitecturas homogéneas y basadas en estándares, que faciliten la gestión centralizada y reduzcan el riesgo de incompatibilidades. “La seguridad no puede ser un mosaico de productos. Necesita coherencia, comunicación y simplicidad”, afirma.

Check Point apuesta por una plataforma de defensa unificada que integra prevención, detección, respuesta y threat intelligence en un mismo entorno. Esto permite aplicar políticas de seguridad coherentes, automatizar tareas repetitivas y mejorar la eficiencia operativa. “La



potencia sin control no sirve de nada. Si no tienes visibilidad, no tienes ciberseguridad”, insiste Nieva.

El factor humano y la cultura de la resiliencia

Además de la tecnología, Nieva destaca el papel del factor humano. “Puedes tener las mejores herramientas, pero si el personal no sabe cómo actuar, el riesgo sigue siendo enorme”.

Por eso, defiende una cultura de ciberresiliencia que implique a toda la organización, desde el consejo de administración hasta los equipos operativos.

Nieva insiste en que la ciberresiliencia no es solo un fin, sino un camino. “Cada incidente ofrece una oportunidad para mejorar. Las empresas que aprenden rápido son las que sobreviven”, concluye. **CST**

Mastercard: “La ciberresiliencia no va solo de tecnología, va de continuidad y confianza”

La ciberresiliencia se ha consolidado como una prioridad estratégica en todas las organizaciones. Así lo defiende Alberto López González, vicepresidente de Cyber Intelligence Solution Product Lead en Mastercard Europa, quien subraya que protegerse no basta: hay que estar preparado para seguir operando cuando todo falla. En esta conversación, analiza la evolución del concepto, los errores más comunes y el papel de la regulación.

Rosalía Arroyo

Errores frecuentes y cambio de mentalidad

Advierte Alberto López que muchas empresas siguen confundiendo ciberseguridad con ciberresiliencia. “No se trata solo de evitar un ataque, sino de ser capaz de continuar y recuperarse”, explica. Esa diferencia, aparentemente semántica, es en realidad estructural: la ciberseguridad protege; la ciberresiliencia garantiza que el negocio no se detenga.

A su juicio, los errores más habituales se repiten: considerar la seguridad como un gasto, dejarla en manos exclusivas del área de TI o ignorar la cadena de suministro, hoy uno de los

“No se trata solo de evitar un ataque, sino de ser capaz de continuar y recuperarse”

eslabones más vulnerables. “No podemos pensar solo en nuestra protección, sino también en la de los proveedores con los que trabajamos”, señala el directivo.

También insiste en la importancia de implicar a todos los niveles de la organización. “La cibe-



Alberto López González, vicepresidente de Cyber Intelligence Solutions en Mastercard Europa

resiliencia empieza en el consejo y termina en cada empleado”, afirma. Para López, la formación y la cultura corporativa son tan importantes

como la tecnología; “una empresa que no entrena a sus equipos es una empresa que corre riesgos innecesarios”.

Tres fases para resistir: antes, durante y después

Mastercard aplica su visión de ciberresiliencia a lo largo de todo el ciclo de vida de un incidente: antes, durante y después del ataque.

En la fase previa, la compañía ayuda a las organizaciones a evaluar su madurez y preparar planes de contingencia. “El primer paso para resistir es saber dónde estás”, recuerda Alberto López, añadiendo que herramientas como RiskRecon, adquirida por Mastercard, permiten analizar de forma continua millones de empresas para detectar vulnerabilidades o configuraciones inseguras en la cadena de suministro.

Durante el incidente, las soluciones basadas en inteligencia artificial y biometría del comportamiento permiten identificar accesos anómalos y detener ataques de fraude o suplantación en tiempo real. Y tras el ataque, los dashboards de análisis forense facilitan el aprendizaje y la mejora continua.



“Nuestra misión es garantizar que los pagos, las operaciones y la confianza no se detengan, incluso en los peores escenarios”, resume López.

Identidad, datos y automatización: el triángulo esencial

En un entorno hiperconectado, la identidad se ha convertido en el nuevo perímetro. “Necesitamos saber quién accede, desde dónde y con qué permisos”, explica el directivo. La gestión de identidades y accesos (IAM) es, por tanto, un componente crítico de la resiliencia: “No se puede proteger lo que no se puede identificar”. Los datos, añade, son “el oro que todos quieren”, y su protección requiere cifrado, redun-

dancia y copias de seguridad inmutables. “El dato no solo tiene valor para quien lo posee, sino también para quien puede usarlo en su contra”.

Por último, la automatización actúa como motor de velocidad. “No podemos depender solo del factor humano. La automatización nos permite reaccionar a la misma velocidad que los atacantes”, afirma. Según López, las organizaciones más resilientes son aquellas que integran automatización, inteligencia artificial y contexto en una estrategia coordinada.

Regulación y madurez del mercado

López reconoce que la regulación ha tenido

un papel decisivo en la madurez de las empresas europeas. “Normativas como GDPR, NIS2, DORA o el Cyber Resilience Act han elevado el listón”, comenta. Estas leyes obligan a las organizaciones a adoptar un enfoque más sistemático, documentado y medible de la ciberseguridad. “Ya no es una opción, es una obligación”, sentencia.

El reto, sin embargo, es ir más allá del cumplimiento formal. Recuerda que “cumplir con la norma no equivale a estar protegido”, y que la ciberresiliencia “implica anticiparse, probar y mejorar de manera continua”.

En este sentido, Mastercard ha reforzado sus equipos de inteligencia de amenazas y ha ampliado su capacidad de análisis en Europa. La compañía monitoriza en tiempo real más de 13 millones de comercios en 200 países y analiza miles de millones de transacciones diarias para detectar patrones de fraude. “Cada dato nos ayuda a proteger mejor a toda la red”, explica Alberto López.

IA como aliada, no como sustituto

“La inteligencia artificial multiplica las amena-



Alberto López González, vicepresidente de Cyber Intelligence Solutions en **Mastercard Europa**

zas, pero también las oportunidades”, afirma López. En Mastercard, la IA se utiliza desde hace más de una década para prevenir el fraude, pero su papel se ha ampliado al ámbito de la detección avanzada y la automatización de la respuesta.

“La IA no ha venido a sustituir a los equipos humanos, sino a potenciar su capacidad de reacción y decisión”, subraya. Al integrar mode-

los de machine learning y análisis predictivo, la compañía es capaz de anticipar comportamientos anómalos y detener incidentes antes de que impacten al usuario final.

Para López, la clave está en combinar tecnología, inteligencia humana y colaboración. “La ciberresiliencia no se construye en solitario. Se construye con alianzas, conocimiento compartido y confianza mutua”, concluye. **CST**

Silverfort: “La identidad es el núcleo de cualquier estrategia de defensa ciberresiliente”

La identidad se ha convertido en el nuevo eje de la seguridad empresarial. Así lo afirma Javier Gómez Berruezo, Territory Manager Iberia de Silverfort, quien analiza en esta entrevista cómo la fragmentación, la automatización y la irrupción de la inteligencia artificial están redefiniendo la ciberresiliencia. En su opinión, solo un enfoque unificado y centrado en la identidad puede garantizar la continuidad del negocio.

Rosalía Arroyo

Para Gómez Berruezo, el mayor error de las organizaciones sigue siendo abordar la seguridad de manera fragmentada. “Tienen silos de soluciones que no se hablan entre sí y dejan puntos ciegos que aprovechan los atacantes”, explica. A menudo, las empresas despliegan múltiples herramientas —de autenticación, gestión de accesos, protección de endpoints o análisis de logs— sin un sistema que las conecte. Esa falta de integración genera lagunas que los ciberdelincuentes explotan con facilidad.

El directivo considera que el perímetro tradicional ha desaparecido, y que hoy el foco debe situarse en la gestión de identidades y accesos.


“El 80 % de los ataques llegan a través de una identidad comprometida”

“El 80 % de los ataques llegan a través de una identidad comprometida”, recuerda. Estas brechas no siempre provienen de errores técnicos, sino de contraseñas débiles, accesos innecesarios o credenciales reutilizadas. “Muchos incidentes podrían evitarse con políticas de autenticación más estrictas y visibilidad sobre quién accede a qué y cuándo”, añade.



Javier Gómez Berruezo,
Territory Manager Iberia de Silverfort

Gómez Berruezo defiende que la ciberresiliencia no es una cuestión de herramientas, sino de coherencia. “Una empresa puede tener las me-



“No podemos esperar horas o días a detener un ataque; hay que hacerlo en ese momento”

jores soluciones, pero si no están coordinadas, sigue estando en riesgo. La resiliencia comienza cuando las capas de seguridad se entienden entre sí y comparten contexto”.

Una visión unificada para anticipar, resistir y recuperarse

Silverfort aborda esta problemática con una plataforma que securiza las identidades de extremo a extremo, tanto humanas como de máquina, en entornos cloud y on-premise. Su propuesta combina visibilidad, control y respuesta automatizada para cubrir los tres momentos

del ciclo de la ciberresiliencia: anticipar, resistir y recuperarse. “Damos visibilidad sobre quién accede, desde dónde y con qué permisos; y somos capaces de bloquear movimientos laterales o escaladas de privilegios en tiempo real”, explica Gómez Berruezo. Esto permite detectar comportamientos anómalos —como accesos simultáneos desde distintas ubicaciones o peticiones inusuales de credenciales— antes de que se produzca una intrusión.

Tras un incidente, la plataforma ofrece información detallada para reconstruir el ataque, evaluar el impacto y fortalecer los controles.

El directivo subraya que esta capacidad de aprendizaje continuo es lo que diferencia a las organizaciones verdaderamente resilientes de las que solo sobreviven. “No se trata de no caer, sino de levantarse rápido, entender lo ocurrido y evitar que se repita”, recuerda Javier Gómez Berruezo.

Automatización y contexto: claves para una defensa viva

“La identidad es el núcleo de cualquier estrategia de defensa”, insiste Gómez Berruezo, recordando que la velocidad de respuesta es lo que marca la diferencia entre un incidente controlado y una brecha devastadora.

Sin embargo, advierte de que la automatización no debe reemplazar la inteligencia humana. “La tecnología detecta patrones, pero sólo las personas entienden el contexto del negocio”. Por eso, Silverfort apuesta por un modelo híbrido en el que las decisiones críticas se basan en la colaboración entre IA y analistas humanos.

El contexto, añade, es tan importante como la detección. “Una alerta sin contexto es ruido. Lo que buscamos es correlacionar datos, entender

qué usuarios están implicados, qué activos se ven afectados y cómo detener la propagación”, explica, añadiendo que la combinación de visibilidad, inteligencia y automatización define una defensa viva: un ecosistema de seguridad que se adapta a los cambios del entorno y aprende de cada intento de ataque.

La madurez del mercado y el nuevo reto de la IA

Aunque reconoce que la conciencia sobre la ciberresiliencia ha crecido, Gómez Berruezo cree que muchas organizaciones siguen reaccionando tarde. “Hay compañías que abren el paraguas cuando ya están mojadas”, ironiza. Los sectores más regulados, como banca, salud o administración pública, son los que más han avanzado, impulsados por marcos normativos como NIS2 o DORA.

Aun así, la ciberresiliencia es un camino continuo. “No basta con cumplir la norma; hay que entenderla, aplicarla y evolucionar con ella”, afirma. De cara al futuro, el directivo destaca un nuevo desafío: los agentes de inteligencia artificial. “Están entre el humano y la máquina, toman



Javier Gómez Berruezo, Territory Manager Iberia de Silverfort

decisiones y ejecutan acciones. Su control será clave desde el punto de vista de la identidad y la visibilidad”, advierte. Estos agentes pueden mejorar la eficiencia de los equipos de seguridad, pero también representan un nuevo vector de riesgo si no están correctamente gestionados. En este escenario, Gómez Berruezo considera que la ciberresiliencia dependerá de la capacidad de armonizar tecnología, procesos y perso-

nas. “La fortaleza de la identidad no es solo técnica, también es cultural. Requiere que todos, desde el CEO hasta el último empleado, comprendan su papel en la protección del negocio”. Para Silverfort, la ciberresiliencia no es un destino, sino una práctica constante de adaptación. Una disciplina que, cuando se centra en la identidad, convierte la seguridad en una ventaja competitiva. **CST**

Sophos: “La ciberresiliencia ya no es una meta, es una forma de trabajar”

La ciberresiliencia ha dejado de ser un objetivo para convertirse en una práctica diaria. Así lo afirma Iván Mateos, Sales Engineer de Sophos Iberia, quien explica cómo la automatización, la identidad y el acompañamiento experto están redefiniendo la protección empresarial. En esta entrevista, analiza el papel del MDR, la madurez del mercado y los nuevos retos que plantea la inteligencia artificial.

Rosalía Arroyo

“Las compañías ya no buscan productos aislados, sino servicios que las respalden las 24 horas”, asegura Iván Mateos, añadiendo que este cambio refleja una transformación profunda en la manera en que las empresas conciben la ciberseguridad. En lugar de centrarse en adquirir herramientas individuales, las organizaciones apuestan por servicios gestionados y enfoques integrales que permitan anticipar, detectar y responder con agilidad ante una amenaza. El directivo explica que el Managed Detection and Response (MDR) se ha convertido en una pieza esencial de esa nueva cultura de resiliencia. “No basta con mirar paneles de alarmas;

“La ciberresiliencia ya no es una meta, es una forma de trabajar”

hace falta un equipo capaz de investigar y actuar antes de que la fiesta comience”, señala. Los servicios MDR de Sophos combinan tecnología avanzada con la supervisión constante de analistas humanos, capaces de correlacionar señales y anticipar ataques antes de que afecten a los sistemas críticos.



Iván Mateos,
Sales Engineer de Sophos Iberia

Iván Mateos resume este nuevo paradigma con claridad: “La ciberresiliencia ya no es una meta, es una forma de trabajar. Implica tener una es-

trategia viva, preparada para responder y evolucionar cada día”.

Identidad, automatización y supervisión continua

En el modelo de Sophos, la identidad ocupa el centro de la estrategia. Cada usuario, dispositivo o servicio puede convertirse en una puerta de entrada al sistema, por lo que la autenticación robusta y la gestión granular de accesos son prioritarias. “La identidad se ha convertido en el nuevo perímetro”, afirma.

El segundo pilar es la automatización, que permite reaccionar en segundos y liberar a los equipos de seguridad de tareas repetitivas. “No podemos depender del factor humano para responder a la velocidad del ataque. La automatización bien aplicada nos da tiempo y eficacia”, explica el directivo.

El tercer pilar es la supervisión continua del riesgo. Sophos combina inteligencia artificial y análisis contextual para ofrecer visibilidad completa sobre vulnerabilidades, comportamiento de usuarios y posibles filtraciones. “A veces lo que para una empresa es leve, para otra puede



ser crítico. Por eso el acompañamiento experto es tan importante como la tecnología”, subraya. La compañía también está impulsando nuevas soluciones como ITDR (Identity Threat Detection and Response), que amplían el alcance del MDR al ámbito de las identidades digitales. En opinión de Iván Mateos, “cada vez más ataques se inician a través de credenciales comprometidas. Las herramientas ITDR son clave para frenar ese vector”.

Más allá del cumplimiento normativo

Mateos valora positivamente el efecto de las regulaciones europeas —NIS2, DORA o el Cyber Resilience Act—, pero advierte que el cumplimiento no debe ser un fin en sí mismo. “Pasar

una auditoría no te hace invulnerable. Atacarte, te van a atacar; la diferencia está en la rapidez y la eficacia de tu respuesta”, señala.

El directivo destaca que estas normativas han contribuido a elevar la madurez del mercado, especialmente en sectores críticos y servicios financieros. Sin embargo, aún percibe brechas entre las grandes corporaciones y las pymes. “En España, muchas pequeñas y medianas empresas carecen de recursos para tener un SOC propio. Por eso la externalización mediante MDR es tan importante: democratiza la ciberresiliencia”.

En esa línea, Sophos ofrece servicios escalables que permiten a cualquier organización acceder a la misma capacidad de detección y respuesta

que una gran empresa, adaptada a su tamaño y presupuesto. “La resiliencia debe ser inclusiva”, apunta el directivo.

La inteligencia artificial, nuevo aliado de la defensa

El avance de la inteligencia artificial (IA) está redefiniendo las operaciones de ciberseguridad. Sophos utiliza IA desde hace más de una década para clasificar y bloquear amenazas, pero los nuevos modelos generativos están multiplicando las posibilidades. “La IA nos permite acelerar la detección, automatizar tareas y apoyar la toma de decisiones en el SOC”, explica Mateos. Los analistas de Sophos trabajan ya con herramientas capaces de interpretar grandes volúmenes de alertas, priorizar incidentes y recomendar acciones en lenguaje natural. “No sustituye al analista, pero lo hace más eficaz”, aclara. Además, la IA ayuda a correlacionar datos dispersos entre endpoints, redes y nubes, creando una visión unificada del entorno. Mateos considera que la IA también exige precaución: “Los atacantes la están usando para mejorar el phishing, automatizar exploits o crear



malware que aprende del entorno. Por eso debemos avanzar al mismo ritmo o más rápido”.

Resiliencia como actitud

Para Mateos, la ciberresiliencia no depende solo de las herramientas, sino de la actitud. “Las empresas verdaderamente resilientes son las que aprenden de cada incidente y mejoran constantemente”, resume, asegurando que la

colaboración con partners tecnológicos, la capacitación continua y la integración de la seguridad en la estrategia de negocio son las claves de ese avance.

En el contexto actual, la resiliencia es el punto de equilibrio entre tecnología, talento y cultura corporativa. “La seguridad ya no se compra; se construye y se mantiene viva cada día”, concluye Iván mateos. 