La preservación inmutable: La nueva categoría que la ciberseguridad no vio venir

Por Oriol Verdura, Vocal de ADSI

Durante décadas, la industria de la seguridad de la información ha operado bajo una premisa casi dogmática: para proteger los activos de una organización, basta con blindar el perímetro digital. Hemos invertido fortunas en cortafuegos de última generación, arquitecturas Zero Trust, cifrado de extremo a extremo y copias de seguridad en la nube con redundancia geográfica. Sin embargo, a medida que las amenazas cibernéticas se vuelven más complejas, un riesgo estructural profundo sigue pasando desapercibido para los comités de dirección y los responsables de ciberseguridad.

Existe un error de base en la gestión de activos estratégicos: **confundimos digitalizar con preservar**. La digitalización es una solución para el presente, pero no está concebida para que prevalezca en el futuro debido a su fragilidad. Los discos duros fallan, los centros de datos consumen ingentes cantidades de energía, los formatos informáticos caducan y el software con el que hoy leemos un documento puede desaparecer en pocas décadas.

Además, en el entorno cibernético actual, las amenazas no se limitan al robo de datos; el *ransomware* masivo, la degradación silenciosa *(bit rot)* y el sabotaje informático han demostrado que cualquier sistema conectado a la red es vulnerable.

A esta fragilidad sistémica se le suma hoy la increíble disrupción de la inteligencia artificial. La IA no solo sintetiza información, sino que rompe la cadena de procedencia al entregar respuestas sin devolver al usuario a la fuente original. En un mundo donde el contenido sintético puede alterar la realidad digital, surge una pregunta crítica para directores de ciberseguridad, responsables de riesgos y custodios de la información: ¿dónde reside la prueba irrefutable de la verdad?. ¿Cómo aseguramos que los datos críticos de un negocio, las patentes de una corporación, los archivos judiciales o el patrimonio cultural de un Estado no han sido alterados, modificados con quién sabe qué fines o borrados para siempre?.



Es en este punto donde nace una nueva categoría conceptual e industrial dentro del ecosistema de la seguridad: la **Seguridad basada en la Preservación Inmutable**.

Esta categoría no pretende competir con las soluciones de ciberseguridad activa ni sustituir el almacenamiento operativo en la nube. Se concibe como un complemento a todo ello. Representa una vuelta de tuerca al concepto clásico de conservación: un nivel extra de protección física y lógica diseñado a prueba de hackers, inmune a los ataques informáticos e independiente de las obsolescencias tecnológicas.

Hasta ahora, la seguridad de la información se ha planteado casi exclusivamente como un problema de código, algoritmos y conectividad. La Seguridad basada en la Preservación rompe esta dependencia al anclar la información en una referencia inmutable sobre un soporte óptico analógico en película fotográfica de 35 milímetros en poliéster de alta estabilidad. Esta tecnología, desarrollada e implementada en infraestructuras como el Centro Integral de Preservación Audiovisual (CIPA) en Málaga de la empresa Preservación 35 (P35), pionera en España, permite convertir cualquier activo digital —datos informáticos, código fuente, archivos audiovisuales o documentos históricos— en un máster analógico inalterable.



¿Por qué esta aproximación constituye un cambio de paradigma para la ciberseguridad global? La respuesta radica en tres pilares fundamentales que ninguna solución puramente digital puede ofrecer simultáneamente:

En primer lugar, superficie de ataque cero y aislamiento absoluto (*air-gap* real). Al convertir los paquetes de datos digitales en un soporte físico fotográfico almacenado en frío (*offline*), el activo queda totalmente desconectado de cualquier red. No existe puerto de entrada, no hay código malicioso que pueda ejecutar instrucciones sobre la película ni *ransomware* capaz de secuestrar la información. Frente a la amenaza de un ciberataque destructivo o un pulso electromagnético, el dato preservado permanece intacto e inaccesible para los atacantes.

En segundo lugar, independencia tecnológica y eliminación de la obsolescencia. Las soluciones de almacenamiento digital tradicionales obligan a realizar migraciones periódicas de datos cada pocos años, lo que genera costes desorbitados, riesgos de migración y degradación silenciosa. El máster analógico de poliéster en 35mm ofrece una vida útil verificable de hasta 500 años sin necesidad de mantenimiento activo, sin consumo energético continuo y con la garantía de ser siempre re-digitalizable en la resolución del futuro sin pérdida de calidad.

En tercer lugar, garantía de autenticidad y soberanía documental. Frente a las trampas de la inteligencia artificial y la falsificación digital, la preservación analógica actúa como el ancla de verdad inmodificable. Ante cualquier litigio legal, auditoría o intento de manipulación en la red, el máster físico se erige en la prueba definitiva contra la que contrastar el dato operativo.

Los directores de seguridad, gestores de riesgos y administraciones públicas no pueden seguir confiando la permanencia de sus activos más críticos a la misma capa digital que está bajo fuego cibernético constante. **Digitalizar produce el presente, pero solo la preservación inmutable garantiza el mañana**. Incorporar este nivel extra de seguridad a prueba de hackers no es un lujo nostálgico, sino el estándar imprescindible para proteger hoy lo que seguirá teniendo valor dentro de quinientos años. ■